E. E. KUMMERS ARBEIT ZU FERMATS LETZTEM SATZ

BACHELORARBEIT VON ALESSANDRO LÄGELER
UNTER DER AUFSICHT VON PROFESSOR RICHARD PINK

1. Einleitung

Fermats letzer Satz, d.i. die Gleichung $x^n + y^n = z^n$ hat keine nichttrivialen ganzzahligen Lösungen für $n \geq 3$, erinnert ein wenig an den Witz: *Gestern Abend habe ich die Lösung für jedes mathematische Problem gefunden, das mit Summen von Primzahlen zu tun hat. Addiere sie nicht.* Wie viele Probleme der Zahlentheorie scheint Fermats letzter Satz mehr *fun fact* zu sein denn wichtiges mathematisches Problem. Ernst Kummer selbst, dessen Beweis im Falle, dass n eine reguläre Primzahl ist, wir in dieser Arbeit darzustellen suchen, hielt den grossen Satz von Fermat für unbedeutend. Freilich ist dessen historische Bedeutung eine Tatsache, doch auch trägt dessen Romantik zu seiner Bekanntheit bei. Ich sage romantisch nicht nur in Hinsicht auf die wohlbekannte Geschichte vom Fermatschen Beweis, der auf dem Rand des Buches keinen Platz hatte, sondern ebenfalls da ein schwieriges mathematisches Problem, das für Laien verständlich ist, von besonderem Reiz ist – gleich eingänglicher Zwölftonmusik.

Diese Arbeit wird nicht den kompletten Beweis darstellen. Ein Lemma, bekannt unter dem Namen *Kummers Lemma*, welches bei weitem der tiefgehendste Teil des Beweises ist, und das wir erst zum Schluss des Beweises an einer unscheinbaren Stelle verwenden, würde die Anzahl Seiten dieser Arbeit mindestens verdoppeln, wenn wir es vollständig beweisen wollten. Wir werden also nicht jeden Schritt in Kummers Lemma ausführen, sondern einige Sätze als gegeben ansehen. Mehr noch, wir gehen einen allgemeineren Weg als nötig, der – so die Hoffnung – dessen Verbindung zur Klassenzahl deutlicher machen soll.

Einige Kenntnisse der kommutativen Algebra, wie man sie zum Beispiel durch die Lektüre von Atiyah und MacDonalds *Introduction to Commutative Algebra* [1] erwirbt, sind vorausgesetzt. Üblicherweise gehören die Beweise der nachfolgenden Sätze zum Standard der algebraischen Zahlentheorie und sind in jedem Buch über dieselbe zu finden. Wir verzichten daher meist auf ein Referenzieren der Art „der Beweis folgt so und so“.

Ich danke Professor Richard Pink für seine Betreuung und seinem Assistenten Nikolas Kuhn für seine zahl- und hilfreichen Kommentare zu früheren Versionen dieser Arbeit.

Zürich, 21. Juli 2016

2. Zahlkörper

Komplexe Zahlen wurden erstmals eingeführt um Nullstellen von Polynomen zu berechnen, ohne besonderes Interesse für die Natur der komplexen Zahlen an sich. Die Rolle der komplexen Zahlen als praktische Notwendigkeit entfachte schnell eine Diskussion über deren Wirklichkeit (man könnte hier die Frage stellen, ob negative ganze Zahlen ein Analogon in der Natur haben); in diesem Sinne wäre es wünschenswert, die „Theorie der komplexen Zahlen“, um einen Ausdruck zu verwenden, den auch Ernst Kummer verwendet hätte, innerhalb der modernen Mathematik zu kontextualisieren; jedoch werden wir komplexe Zahlen wie in ihrem Ursprung hauptsächlich als Werkzeug ansehen. Möglicherweise wird einiges wenig motiviert, alleine-stehend scheinen. Dies angemerkt, beginnen wir sogleich mit der Wiederholung einiger algebraischer Konzepte:

Unter einem Zahlkörper verstehen wir eine endliche Körpererweiterung der rationalen Zahlen $\mathbf{Q}$. Zum Beispiel ist für eine positive ganze Zahl n der n-te Kreisteilungskörper $\mathbf{Q}(\xi_n)$ mit $\xi_n := \exp\left(\frac{2\pi i}{n}\right)$ ein Zahlkörper, denn ξ_n ist als Nullstelle von $X^n - 1$ algebraisch.

Gegeben zwei Ringe $B \supset A$, wobei *Ring* stets kommutativer Ring mit Einselement bedeuten soll, heisst ein Element $x \in B$ *ganz über* A, falls x Nullstelle eines normierten Polynoms mit Koeffizienten in A ist. Die Menge aller ganzen Elemente über A heisst der *ganze Abschluss* von A in B und bildet einen Unterring von B. Im Falle eines Zahlkörpers K nennen wir den ganzen Abschluss des Unterringes $\mathbf{Z}$ den *Ring der ganzen Zahlen* von K und dessen Elemente *algebraische ganze Zahlen*. Der Ring der ganzen Zahlen des Zahlkörpers $\mathbf{Q}$ ist $\mathbf{Z}$.

Da ξ_n Nullstelle von $X^n - 1$ ist, enthält der Ring der ganzen Zahlen von $\mathbf{Q}(\xi_n)$ den Ring $\mathbf{Z}[\xi_n]$. Tatsächlich ist der Ring der ganzen Zahlen von $\mathbf{Q}(\xi_n)$ gleich $\mathbf{Z}[\xi_n]$; wir werden dies später in dem für uns relevanten Spezialfall beweisen.

Sei μ_n die Gruppe der Nullstellen von $X^n - 1$. Die von ξ_n erzeugte zyklische Gruppe $\langle \xi_n \rangle$ ist eine Untergruppe von μ_n. Da $\xi_n^i - \xi_n^j = \xi_n^i(1 - \xi_n^{j-i}) \neq 0$ ist für alle $0 \leq i, j < n$ und $i \neq j$, ist die Ordnung von $\langle \xi_n \rangle$ gleich n. Da die Ordnung von μ_n gleich n ist, ist $\mu_n = \langle \xi_n \rangle$.

Wegen der Faktorisierung $X^n - 1 = \prod_{k=0}^{n-1}(X - \xi_n^k)$ ist $\mathbf{Q}(\xi_n)$ der Zerfällungskörper des Polynoms $X^n - 1$ über $\mathbf{Q}$; insbesondere ist $\mathbf{Q}(\xi_n)/\mathbf{Q}$ eine normale Erweiterung.

Ein Element σ aus $\mathrm{Gal}(\mathbf{Q}(\xi_n)/\mathbf{Q})$ muss ξ_n auf einen Erzeuger von μ_n (eine sogenannte *primitive* n-te Einheitswurzel) abbilden. Die Erzeuger von μ_n sind genau ξ_n^i für alle $i \geq 0$ mit $\mathrm{ggT}(n, i) = 1$. Folglich ist $[\mathbf{Q}(\xi_n) : \mathbf{Q}] = |\mathrm{Gal}(\mathbf{Q}(\xi_n)/\mathbf{Q})| \leq \varphi(n)$ mit $\varphi(n) = \left| (\mathbf{Z}/n\mathbf{Z})^\times \right|$ der Eulerschen φ-Funktion.

Sei p eine Primzahl. Da das Polynom

$$\frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + ... + X + 1 = \prod_{k=1}^{p-1}(X - \xi_p^k)$$

normiert und vom Grad $p-1 = \varphi(p) = [\mathbf{Q}(\xi_p) : \mathbf{Q}]$ ist, ist es das Minimalpolynom von ξ_p und insbesondere irreduzibel. Allgemeiner können wir das n-te Kreisteilungspolynom $\Phi_n = \prod_\xi (X - \xi)$ definieren, wobei das Produkt über die primitiven n-ten Einheitswurzeln ξ gebildet wird. Das n-te Kreisteilungspolynom hat ganzzahlige Koeffizienten:

Lemma 2.1. *Das Minimalpolynom einer algebraischen ganzen Zahl hat ganzzahlige Koeffizienten.*

Beweis. Sei K ein Zahlkörper und α ganz in K. Sei $f = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ mit $a_0, ..., a_n \in \mathbf{Q}$ das Minimalpolynom von α über $\mathbf{Q}$ und sei L der Zerfällungskörper von f über K. Sei g ein normiertes Polynom mit ganzzahligen Koeffizienten, so dass α eine Nullstelle von g ist. Dann teilt f das Polynom g und somit sind alle weiteren Nullstellen $\alpha_1, ..., \alpha_{n-1}$ von f ebenfalls ganz im Zahlkörper L. Die Koeffizienten von f sind Polynome in $\alpha, \alpha_1, ..., \alpha_{n-1}$, und da die algebraischen ganzen Zahlen einen Ring bilden, sind die Koeffizienten von f algebraische ganze Zahlen. Da $a_0, ..., a_{n-1}$ auch rationale Zahlen sind, müssen sie in $\mathbf{Z}$ liegen. □

Satz 2.2. *Für jede positive ganze Zahl n ist das Polynom Φ_n irreduzibel über $\mathbf{Q}$.*

Beweis. Für die Irreduzibilität von Φ_n ist wegen Lemma 2.1 nur zu zeigen, dass Φ_n keine nicht-konstanten echten Faktoren mit ganzzahligen Koeffizienten hat.

Sei f also ein nicht-konstanter normierter Faktor von Φ_n mit ganzzahligen Koeffizienten und α eine primitive n-te Einheitswurzel, welche Nullstelle von f ist. Wir beweisen, dass für jede zu n teilerfremde Primzahl p die p-te Potenz α^p eine weitere Nullstelle von f ist. Dies ist ausreichend, um Satz 2.1 zu beweisen: Wenn k eine zu n teilerfremde positive ganze Zahl ist, so besteht deren Primfaktorisierung $k = p_1 \cdots p_m$ mit $m \in \mathbf{Z}_{>0}$ aus zu n teilerfremden Primzahlen p_i und damit ist $\alpha^k = \alpha^{p_1 \cdots p_m}$ induktiv ebenso eine Nullstelle von f. Jedoch ist jede weitere primitive n-te Einheitswurzel durch α^k mit $1 \leq k < n$ und $\mathrm{ggT}(k, n) = 1$ gegeben und somit muss $f = \Phi_n$ sein.

Wenn wir im Polynom $\prod_{k=1}^{n-1}(X - \alpha^k) = X^{n-1} + X^{n-2} + ... + X + 1$ für X die Zahl 1 substituieren, erhalten wir n. Wenn wir für X die Zahl 0 substituieren, ergibt sich $\prod_{k=1}^{n-1}(-\alpha^k) = (-1)^{n-1}\prod_{k=1}^{n-1}\alpha^k = 1$. Wir betrachten

$$\begin{aligned}\Delta &:= \prod_{1\leq i<j\leq n}(\alpha^i - \alpha^j)^2 = (-1)^{\frac{1}{2}(n-1)n}\prod_{i\neq j}(\alpha^i - \alpha^j) \qquad (2.1)\\ &= (-1)^{\frac{1}{2}(n-1)n}\prod_{i\neq j}\alpha^i(1-\alpha^{j-i}) = (-1)^{\frac{1}{2}(n-1)n}\prod_{i=0}^{n-1}\alpha^i\left(\prod_{k=1}^{n-1}\left(1-\alpha^k\right)\right)\\ &= n^n(-1)^{\frac{1}{2}(n-1)n}\prod_{i=0}^{n-1}\alpha^i = (-1)^{\frac{1}{2}(n+1)n+1}n^n.\end{aligned}$$

Sei widerspruchsweise p eine Primzahl, die n nicht teilt, und so, dass α^p keine Nullstelle von f ist; dann ist $f(\alpha^p) \neq 0$ eine algebraische ganze Zahl, die auch noch $\Delta = \pm n^n$ (als algebraische ganze Zahl) teilt. Es ist $f(\alpha^p) \equiv f(\alpha)^p = 0 \pmod{p}$ und somit ist p ein Teiler von n^n (als algebraische ganze Zahl).

Sei $\beta \in \mathbf{Q}(\xi_n)$ eine algebraische ganze Zahl, so dass $n^n = p \cdot \beta$ ist. Dann ist $\beta = \frac{n^n}{p} \in \mathbf{Q}$ ganz über $\mathbf{Z}$ und damit ist $\beta \in \mathbf{Z}$. Dieser Widerspruch zur Teilerfremdheit von p und n beweist, dass α^p eine weitere Nullstelle von f sein muss, was wiederum Satz 2.1 beweist. Der eben gegebene Beweis geht auf Issai Schur zurück [2]. □

Satz 2.2 zeigt insbesondere auch, dass $[\mathbf{Q}(\xi_n) : \mathbf{Q}] = \varphi(n)$, da Φ_n das Minimalpolynom von ξ_n über $\mathbf{Q}$ und vom Grad $\varphi(n)$ ist.

Ein Ideal eines Ringes A ist schlicht ein A-Untermodul von A. Wenn K ein Zahlkörper ist und A dessen Ring der ganzen Zahlen, dann bezeichnen wir als *gebrochenes Ideal* einen A-Untermodul $M \neq 0$ von K mit der Eigenschaft, dass ein $x \in K^\times$ existiert, so dass $xM \subset A$ ist. Jedes Ideal von A ist ein

gebrochenes Ideal von K, ebenso ist yA für jedes $y \in K^\times$ ein gebrochenes Ideal von K. Für gewöhnlich werden wir schlicht „Ideal in K“ sagen, wenn wir über gebrochene Ideale sprechen wollen; letzteres Beispiel sei ein „Hauptideal in K“.

Wie zum Beispiel in [1, Kap. 9] gezeigt wird, ist der Ring der ganzen Zahlen eines Zahlkörpers K ein Dedekindring. Die Ideale in K bilden eine multiplikative Gruppe J_K, wobei für zwei Ideale M, N in K mit $M \cdot N$ das von $\{ab : a \in M, b \in N\}$ erzeugte Ideal in K gemeint ist. Das Einselement von J_K ist A. Sei P die Untergruppe der Hauptideale in K. Der Quotient $H_K = J_K/P$ heisst die *Klassengruppe* von K. Da für jedes $M \in J_K$ ein $x \in K^\times$ existiert, so dass $xM \subset A$ ist, enthält jede Nebenklasse $M \cdot P$ in H_K ein Ideal in A.

Da A ein Dedekindring ist, kann jedes Ideal $\mathfrak{a} \neq 0$ in A als eindeutiges Produkt von Primidealen $\mathfrak{a} = \prod \mathfrak{p}^{n(\mathfrak{p})}$ (eindeutig bis auf Umordnung) mit $n(\mathfrak{p}) \geq 0$, fast alle Null, geschrieben werden. Der Ring A ist eindimensional, d.h. jedes Primideal, das nicht Null ist, ist maximal, und mithin sind die Primideale, die nicht Null sind, paarweise koprim. Wenn also $\mathfrak{b} = \prod \mathfrak{p}^{m(\mathfrak{p})}$ ein in $\mathfrak{a}$ enthaltenes Ideal sei, so gilt $\mathfrak{a}^{-1}\mathfrak{b} = \prod \mathfrak{p}^{m(\mathfrak{p})-n(\mathfrak{p})} \subset \mathfrak{a}^{-1}\mathfrak{a} = A$ (siehe z.B. [3, VII.3]) mit $m(\mathfrak{p}) - n(\mathfrak{p}) \geq 0$ fast alle Null. Für alle $\alpha \in \mathfrak{a}$ existiert ein Ideal $\mathfrak{c}$ in A mit $\mathfrak{a}\mathfrak{c} = (\alpha)$.

3. Der Ring $\mathbf{Z}[\xi_p]$

In diesem Abschnitt sei p stets eine ungerade Primzahl und ξ stets eine primitive p-te Einheitswurzel. Der Zahlkörper, der uns im folgenden hauptsächlich interessieren wird, ist der p-te Kreisteilungskörper. Betrachten wir die Gleichung $x^p + y^p = z^p$ als Gleichung von Elementen $x, y, z \in \mathbf{Z}[\xi]$, so können wir

$$z^p = x^p + y^p = (x+y)(x+\xi y)(x+\xi^2 y)\cdots(x+\xi^{p-1}y)$$

schreiben. Diesen Ansatz verfolgte schon Gabriel Lamé, welcher einen falschen Beweis zu Fermats letztem Satz schrieb, indem er annahm, dass der Ring $\mathbf{Z}[\xi]$ faktoriell sei (einen ähnlichen Fehler beging schon Euler, doch davon später). Dies ist im Allgemeinen nicht der Fall.

Wir werden uns, da das Problem nun „multiplikativ“ ist, etwas mehr mit der Einheitengruppe des Ringes $\mathbf{Z}[\xi]$ beschäftigen müssen.

Lemma 3.1. *Für alle $1 \leq i, j \leq p-1$ ist $\frac{1-\xi^i}{1-\xi^j}$ eine Einheit in $\mathbf{Z}[\xi]$.*

Beweis. Wir brauchen einzig zu zeigen, dass $\frac{1-\xi^i}{1-\xi^j}$ für alle $i, j \in \{1, ..., p-1\}$ in $\mathbf{Z}[\xi]$ liegt; dann ist nämlich auch $\left(\frac{1-\xi^i}{1-\xi^j}\right)^{-1} = \frac{1-\xi^j}{1-\xi^i} \in \mathbf{Z}[\xi]$. Da das Bild von j unter der kanonischen Abbildung $\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ die Gruppe $\mathbf{Z}/p\mathbf{Z}$ erzeugt, existiert eine ganze Zahl $t > 0$, so dass $tj \equiv i \pmod{p}$ ist und damit

$$\xi^i - 1 = \xi^{tj} - 1 = (\xi^j - 1)(\xi^{j(t-1)} + ... + \xi^j + 1).$$

□

Wenn wir im Polynom $X^{p-1} + X^{p-2} + ... + X + 1 = \prod_{k=1}^{p-1}(X - \xi^k)$ wie schon vorhin für X die Zahl 1 substituieren, bekommen wir $p = \prod_{k=1}^{p-1}(1 - \xi^k)$. Aus Lemma 3.1 folgt die Existenz einer Einheit u in $\mathbf{Z}[\xi]$, so dass $p = u(1-\xi)^{p-1}$ ist. Bezeichne von jetzt an $(1-\xi)$ stets das von $1-\xi$ erzeugte Hauptideal im Ring der ganzen Zahlen B von $\mathbf{Q}(\xi)$. Dann gilt $pB = (1-\xi)^{p-1}$.

Für jede ganze Zahl m, die in $(1-\xi)$ liegt, folgt, dass m^{p-1} in $(1-\xi)^{p-1} = pB$ liegt und also dass p die ganze Zahl m als ganze Zahl teilt. Wir halten fest, dass eine ganze Zahl genau dann in $(1-\xi)$ liegt, wenn sie durch p teilbar ist.

Sei K ein Zahlkörper und A dessen Ring der ganzen Zahlen. Für ein Primideal $\mathfrak{p} \neq 0$ in $\mathbf{Z}$ können wir $\mathfrak{p}A = \prod \mathfrak{P}^{e(\mathfrak{P})}$ schreiben, wobei $\mathfrak{P}$ Primideale in A und $e(\mathfrak{P}) \geq 0$ fast alle Null sind. Wir sagen, dass ein Ideal $\mathfrak{P}$ mit $e(\mathfrak{P}) \geq 1$ das Ideal $\mathfrak{p}$ *teilt* und schreiben $\mathfrak{P} \mid \mathfrak{p}$. Falls $e(\mathfrak{P}) > 1$ ist für ein $\mathfrak{P}$, so heisst $\mathfrak{p}$ *verzweigt* und andernfalls *unverzweigt*. Dies überträgt sich analog auf endliche Erweiterungen von Zahlkörpern L/K und wir nennen eine solche *unverzweigt*, falls alle Primideale im Ring der ganzen Zahlen von K unverzweigt sind.

Falls ein Primideal $\mathfrak{P}$ in A ein Primideal $\mathfrak{p} \neq 0$ in $\mathbf{Z}$ teilt, so gilt offenbar $\mathfrak{P} \cap \mathbf{Z} \supset \mathfrak{p}$. Weil $\mathfrak{P} \cap \mathbf{Z}$ als Urbild von $\mathfrak{P}$ unter dem Einbettungshomomorphismus $\mathbf{Z} \hookrightarrow A$ selbst prim und weil jedes Primideal in $\mathbf{Z}$ maximal ist, muss $\mathfrak{p} = \mathfrak{P} \cap \mathbf{Z}$ gelten. Folglich kann $\mathbf{Z}/\mathfrak{p}$ in $A/\mathfrak{P}$ eingebettet werden. Wir schreiben $f(\mathfrak{P})$ für den Grad $[A/\mathfrak{P} : \mathbf{Z}/\mathfrak{p}]$.

Satz 3.2. *Sei K ein Zahlkörper und A dessen Ring der ganzen Zahlen. Sei $\mathfrak{p}$ ein maximales Ideal in $\mathbf{Z}$. Dann ist*

$$[K : \mathbf{Q}] = \sum_{\mathfrak{P}\mid\mathfrak{p}} e(\mathfrak{P}) f(\mathfrak{P}),$$

wobei wir über die maximalen Ideale $\mathfrak{P}$ in A summieren.

Beweis. Sei $n := [K : \mathbf{Q}]$. Es existiert eine $\mathbf{Q}$-Basis $w_1, ..., w_n$ von K, so dass A in $\mathbf{Z}w_1 + ... + \mathbf{Z}w_n$ enthalten ist (siehe [1, Prop. 5.17]). Da $\mathbf{Z}$ ein noetherscher Ring ist und da A ein $\mathbf{Z}$-Untermodul des freien $\mathbf{Z}$-Moduls $\mathbf{Z}w_1 + ... + \mathbf{Z}w_n$ ist, ist A ein endlich erzeugter $\mathbf{Z}$-Modul. Ein torsionsfreier, endlich erzeugter Modul über einem Hauptidealring ist ein freier Modul von endlichem Rang [4, VII.15 Cor.2], also ist A ein freier $\mathbf{Z}$-Modul. Sei m der Rang des freien $\mathbf{Z}$-Moduls A.

Es ist $(\mathbf{Z} - \{0\})^{-1}A = K$, da jedes Element in K multipliziert mit dem Hauptnenner der Koeffizienten seines Minimalpolynoms in A liegt. Insbesondere können wir die Elemente jeder $\mathbf{Q}$-Basis in K so mit Skalaren multiplizieren, dass die sich ergebende Basis in A liegt.

Wir haben

$$K = (\mathbf{Z} - \{0\})^{-1}A \cong (\mathbf{Z} - \{0\})^{-1} \bigoplus_{i=1}^{m} \mathbf{Z} \cong \bigoplus_{i=1}^{m} \mathbf{Q}$$

als $\mathbf{Q}$-Vektorräume und damit folgt $m = \dim_{\mathbf{Q}} K$.

Lokalisieren wir nun $\mathbf{Z}$ an $\mathfrak{p}$ und schreiben $A_\mathfrak{p}$ für $A \otimes_{\mathbf{Z}} \mathbf{Z}_\mathfrak{p}$, so ist $A_\mathfrak{p}$ ein freier Modul vom Rang n über $\mathbf{Z}_\mathfrak{p}$. Sei $\mathfrak{P}$ ein Primideal in $A_\mathfrak{p}$. Für ein Primideal $\mathfrak{P}$ in A schreiben wir $\hat{\mathfrak{P}} := A_\mathfrak{p}\mathfrak{P}$ und $\hat{\mathfrak{p}}$ für das maximale Ideal in $\mathbf{Z}_\mathfrak{p}$. Der Ring $A_\mathfrak{p}$ enthält genau die Primideale $\hat{\mathfrak{P}}$, welche zu jenen Primidealen $\mathfrak{P}$ gehören, die $\mathfrak{p}$ teilen. Der $\mathbf{Z}_\mathfrak{p}/\hat{\mathfrak{p}}$-Vektorraum $A_\mathfrak{p}/\hat{\mathfrak{p}}A_\mathfrak{p}$ hat Dimension n.

En effet, die exakte Sequenz

$$0 \to \hat{\mathfrak{p}} \to \mathbf{Z}_\mathfrak{p} \to \mathbf{Z}_\mathfrak{p}/\hat{\mathfrak{p}} \to 0$$

von $\mathbf{Z}_\mathfrak{p}$-Moduln induziert die exakte Sequenz

$$\hat{\mathfrak{p}} \otimes_{\mathbf{Z}_\mathfrak{p}} A_\mathfrak{p} \to \mathbf{Z}_\mathfrak{p} \otimes_{\mathbf{Z}_\mathfrak{p}} A_\mathfrak{p} \to (\mathbf{Z}_\mathfrak{p}/\hat{\mathfrak{p}}) \otimes_{\mathbf{Z}_\mathfrak{p}} A_\mathfrak{p} \to 0$$

von $\mathbf{Z}_\mathfrak{p}$-Moduln [1, Prop. 2.18.] und also ist $A_\mathfrak{p}/\hat{\mathfrak{p}}A_\mathfrak{p} \cong (\mathbf{Z}_\mathfrak{p}/\hat{\mathfrak{p}}) \otimes_{\mathbf{Z}_\mathfrak{p}} A_\mathfrak{p}$ wegen [1, Prop. 2.14.iv]. Da $A_\mathfrak{p}$ als $\mathbf{Z}_\mathfrak{p}$-Modul Rang n hat, folgt $\dim_{\mathbf{Z}_\mathfrak{p}/\hat{\mathfrak{p}}} \left((\mathbf{Z}_\mathfrak{p}/\hat{\mathfrak{p}}) \otimes_{\mathbf{Z}_\mathfrak{p}} A_\mathfrak{p}\right) = n$.

Wir schreiben nun $K' := \mathbf{Z}_\mathfrak{p}/\hat{\mathfrak{p}}$, um die Notation etwas übersichtlicher zu gestalten. Um Satz 3.2 zu beweisen, ist es nach den vorherigen Betrachtungen ausreichend, wenn wir $\dim_{K'} A_\mathfrak{p}/\hat{\mathfrak{p}}A_\mathfrak{p} = \sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P})f(\mathfrak{P})$ zeigen. Dazu beweisen wir das folgende Lemma:

Lemma 3.3. *Ein Dedekindring, der nur endlich viele Primideale enthält, ist ein Hauptidealring.*

Beweis. Sei A ein solcher Dedekindring und seien $\mathfrak{q}_1, ..., \mathfrak{q}_s$ die endlich vielen paarweise verschiedenen maximalen Ideale in A. Sei $\mathfrak{a} \neq 0$ ein Ideal und sei $\mathfrak{a} = \mathfrak{q}_1^{m_1} \cdots \mathfrak{q}_s^{m_s}$. Nach dem Chinesischen Restsatz haben wir einen surjektiven Homomorphismus

$$A \to \prod_{i=1}^{s} A/\mathfrak{q}_i^{m_i+1}.$$

Für einen beliebigen endlich erzeugten Modul M über A gilt $\mathfrak{a}M = M$ für ein Ideal $\mathfrak{a}$ von A genau dann, wenn ein $a \in \mathfrak{a}$ existiert, so dass $(1+a)M = 0$ ist [3, II 2.2 Cor. 3]. Da A ein Dedekindring ist, ist $\mathfrak{q}_i$ ein endlich erzeugter A-Modul. Wäre $\mathfrak{q}_i = \mathfrak{q}_i^2$, so existierte also ein Element $e \in \mathfrak{q}_i$ mit $a \cdot e = a$ für alle $a \in \mathfrak{q}_i$. Dies aber gibt $e^2 = e$ und damit $e = 0, 1$ im Widerspruch dazu, dass alle $\mathfrak{q}_i$ prim und nicht Null sind. Also muss $\mathfrak{q}_i \neq \mathfrak{q}_i^2$ sein. Sei π_i ein Element aus $\mathfrak{q}_i$, welches nicht in $\mathfrak{q}_i^2$ liegt.

Die Surjektion $A \to \prod_{i=1}^{s} A/\mathfrak{q}_i^{m_i+1}$ gibt uns ein Element $\alpha \in A$, so dass $\alpha \equiv \pi_r^{m_i} \not\equiv 0 \pmod{\mathfrak{q}_i^{m_i+1}}$ ist für alle $1 \leq i \leq s$. Dies impliziert $(\alpha) \supset \mathfrak{a}$, da in der Primfaktorisierung des Ideals $(\alpha) = \mathfrak{q}_1^{m_1'} \cdots \mathfrak{q}_s^{m_s'}$ für alle i gilt, dass $m_i' \leq m_i$ ist. Jedoch ist $\alpha \in \mathfrak{q}_1^{m_1} \cap ... \cap \mathfrak{q}_s^{m_s} = \mathfrak{a}$, da $\alpha \equiv \pi_i^{m_i} \equiv 0 \pmod{\mathfrak{q}_i^{m_i}}$ für alle i ist, und damit folgt $\mathfrak{a} = (\alpha)$. □

Kehren wir zurück zum Beweis von Satz 3.2: Sei ω ein Erzeuger des Hauptideals $\hat{\mathfrak{P}}$ in $A_\mathfrak{p}$. Der Ring $A_\mathfrak{p}/\hat{\mathfrak{P}}^e$ ist ein lokaler Ring mit Primideal $\hat{\mathfrak{P}}$ für jedes $e > 1$. Die Dimension von $A_\mathfrak{p}/\hat{\mathfrak{P}}^e$ als K'-Vektorraum ist die Länge einer Kompositionsreihe [1, Prop. 6.7]. Wenn wir die Kette $A_\mathfrak{p} \supset \hat{\mathfrak{P}} \supset \hat{\mathfrak{P}}^2 \supset \cdots \supset \hat{\mathfrak{P}}^e$ betrachten, ersehen wir

$$\dim_{K'} \left(A_\mathfrak{p}/\hat{\mathfrak{P}}^e\right) = \sum_{l=0}^{e-1} \dim_{K'} \left(\hat{\mathfrak{P}}^l/\hat{\mathfrak{P}}^{l+1}\right).$$

Die Komposition $A_\mathfrak{p} \to \hat{\mathfrak{P}}^l \to \hat{\mathfrak{P}}^l/\hat{\mathfrak{P}}^{l+1}$, wobei die erste Abbildung Multiplikation mit ω^l und die zweite die kanonische Quotientenabbildung ist, induziert einen Isomorphismus $A_\mathfrak{p}/\hat{\mathfrak{P}} \cong \hat{\mathfrak{P}}^l/\hat{\mathfrak{P}}^{l+1}$ von K'-Vektorräumen. Damit ist

$$\dim_{K'} \left(A_\mathfrak{p}/\hat{\mathfrak{P}}^e\right) = \sum_{l=0}^{e-1} \dim_{K'} \left(A_\mathfrak{p}/\hat{\mathfrak{P}}\right) = e \dim_{K'} \left(A_\mathfrak{p}/\hat{\mathfrak{P}}\right)$$

Nun ist aber $f(\mathfrak{P}) = \dim_{K'} \left(A_\mathfrak{p}/\hat{\mathfrak{P}}\right)$. Mit dem Chinesischen Restsatz folgt für $\hat{\mathfrak{p}}A_\mathfrak{p} = \prod_{\mathfrak{P}} \hat{\mathfrak{P}}^{e(\mathfrak{P})}$, dass

$$A_\mathfrak{p}/\hat{\mathfrak{p}}A_\mathfrak{p} \cong \prod_{\mathfrak{P}} A_\mathfrak{p}/\hat{\mathfrak{P}}^{e(\mathfrak{P})}$$

und $\dim_{K'} (A_\mathfrak{p}/\hat{\mathfrak{p}}A_\mathfrak{p}) = \sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P})f(\mathfrak{P})$ ist. Damit ist Satz 3.2 bewiesen. □

Der eben bewiesene Satz zeigt auch, dass $(1-\xi)$ ein Primideal ist; denn wäre $(1-\xi)$ kein Primideal, so wäre

$$\sum_{\mathfrak{P}|p\mathbf{Z}} e(\mathfrak{P})f(\mathfrak{P}) \geq (p-1)\sum_{\mathfrak{Q}} r(\mathfrak{Q}) > p-1 = [\mathbf{Q}(\xi):\mathbf{Q}],$$

wobei die Summe in $\mathfrak{Q}$ über die Primideale von A geht, die in der Faktorisierung $\prod_{\mathfrak{Q}} \mathfrak{Q}^{r(\mathfrak{Q})}$ von $(1-\xi)$ vorkommen. Weiter noch:

Korollar 3.4. *Sei B der Ring der ganzen Zahlen von $\mathbf{Q}(\xi)$. Dann ist*

$$B/(1-\xi)B \cong \mathbf{Z}/p\mathbf{Z}.$$

Insbesondere ist jedes Element von B kongruent zu einer ganzen Zahl modulo $(1-\xi)$.

Beweis. Nach dem letzten Satz gilt $f((1-\xi))=1$, da

$$[\mathbf{Q}(\xi):\mathbf{Q}] = \sum_{\mathfrak{P}|p\mathbf{Z}} e(\mathfrak{P})f(\mathfrak{P}) = e((1-\xi))f((1-\xi)) = (p-1)\cdot f((1-\xi))$$

ist. Somit ist Körpererweiterung $B/(1-\xi)B$ über $\mathbf{Z}/p\mathbf{Z}$ trivial. □

Wir wollen nun beweisen, dass der Ring der ganzen Zahlen B von $\mathbf{Q}(\xi)$ gleich $\mathbf{Z}[\xi]$ ist. Korollar 3.4 impliziert, dass

$$(\mathbf{Z}+(1-\xi)B)/(1-\xi)B \cong \mathbf{Z}/((1-\xi)B\cap\mathbf{Z}) = \mathbf{Z}/p\mathbf{Z} \cong B/(1-\xi)B$$

sind als $\mathbf{Z}$-Moduln. Für Moduln $L \supset M \supset N$ über einen beliebigen Ring gilt $(L/N)/(M/N) \cong L/M$ [1, Prop. 2.1.i]. Daraus folgt

$$0 = ((\mathbf{Z}+(1-\xi)B)/(1-\xi)B) \,/\, (B/(1-\xi)B) \cong (\mathbf{Z}+(1-\xi)B)/B,$$

und also $B = \mathbf{Z}+(1-\xi)B$. Weiter ist auch $B = \mathbf{Z}+(1-\xi)B \subset \mathbf{Z}[\xi]+(1-\xi)B \subset B$ und

$$B = \mathbf{Z}[\xi]+(1-\xi)B = \mathbf{Z}[\xi]+(1-\xi)\mathbf{Z}[\xi]+(1-\xi)^2B = \mathbf{Z}[\xi]+(1-\xi)^2B.$$

Per Induktion folgt dann

$$B = (1-\xi)B+\mathbf{Z}[\xi] = (1-\xi)^2B+\mathbf{Z}[\xi] = \ldots = (1-\xi)^kB+\mathbf{Z}[\xi]$$

für jede positive ganze Zahl k.

Die *Diskriminante* $D(v_1,\ldots,v_n)$ einer $\mathbf{Q}$-Basis $v_1,\ldots,v_n$ eines Zahlkörpers K vom Grad n ist als $\det\left((\sigma_i(v_j))_{i,j}\right)^2$ definiert, wobei $\sigma_1,\ldots,\sigma_n$ die verschiedenen $\mathbf{Q}$-Einbettungen in $\mathbf{C}$ sind, d.h. die Elemente der Galois-Gruppe verknüpft mit einer Einbettung von K in $\mathbf{C}$. Die Diskriminante ist invariant unter der Nummerierung der Einbettungen und der Basis, da die Determinante bis aufs Vorzeichen invariant ist, wenn wir Spalten oder Zeilen der Matrix vertauschen. Jedoch ist die Diskriminante im Allgemeinen nicht unabhängig von der Wahl der Basis von K.

Als Beispiel berechnen wir die Diskriminante der Basis $1,\xi,\xi^2,\ldots,\xi^{p-2}$ von $\mathbf{Q}(\xi)$. Wir indizieren die Elemente von $\mathrm{Gal}(\mathbf{Q}(\xi)/\mathbf{Q})$ so, dass $\sigma_i(\xi)=\xi^i$ ist für alle $1\leq i\leq p-1$.

Dann ist $D(1,\xi,\xi^2,...,\xi^{p-2}) = \det\left((\xi^{(j-1)i})_{i,j}\right)^2$ die Determinante einer Vandermonde-Matrix, nämlich

$$D(1,\xi,\xi^2,...,\xi^{p-2}) = \prod_{0\le i<j\le p-2}(\xi^j-\xi^i)^2 = \frac{\prod_{1\le i<j\le p}(\xi^j-\xi^i)^2}{\prod_{k=1}^{p-1}(1-\xi^k)^2} = \frac{\pm p^p}{\left(\prod_{k=1}^{p-1}(1-\xi^k)\right)^2} = \pm p^{p-2} \tag{3.1}$$

nach Gleichung (2.1).

Satz 3.5. *Der Ring der ganzen Zahlen B von $\mathbf{Q}(\xi)$ ist $\mathbf{Z}[\xi]$.*

Beweis. Sei D die Diskriminante der Basis $1,\xi,\xi^2,...,\xi^{p-2}$. Für $\alpha = a_0 + a_1\xi + ... + a_{p-2}\xi^{p-2}$ mit $a_0,...,a_{p-2} \in \mathbf{Q}$ ist

$$\mathrm{Tr}(\alpha\xi^i) = \sum_{j=0}^{p-2}\mathrm{Tr}(\xi^j\xi^i)a_j \in \mathbf{Q}$$

für alle $1 \le i \le p-2$. Sei γ die Matrix $(\mathrm{Tr}(\xi^{(j-1)i}))_{i,j} = \left((\xi^{(j-1)i})_{i,j}\right)^2$. Wir haben

$$\gamma^{-1}\left(\mathrm{Tr}(\alpha\xi^i)\right)_i = \frac{1}{D}\mathrm{adj}(\gamma)\left(\mathrm{Tr}(\alpha\xi^i)\right)_i = (a_i)_i$$

Die Adjunkte $\mathrm{adj}(\gamma)$ liegt in $\mathbf{Z}^{(p-1)\times(p-1)}$ und $\mathrm{Tr}(\alpha\xi^i)$ liegt in $\mathbf{Z}$. Folglich ist $D\cdot B \subset \mathbf{Z}[\xi]$. Wenn wir nun für k in der Gleichung $B = (1-\xi)^k B + \mathbf{Z}[\xi]$ die Zahl $(p-1)(p-2)$ einsetzen, dann folgt

$$B = p^{p-2}B + \mathbf{Z}[\xi] \subset \mathbf{Z}[\xi].$$

□

Die Basis $1,\xi,\xi^2,...,\xi^{p-2}$ hat die Eigenschaft, dass sie auch $\mathbf{Z}[\xi]$ als $\mathbf{Z}$-Modul erzeugt. Eine $\mathbf{Q}$-Basis $v_1,...,v_n$ eines Zahlkörpers K mit $n := [K:\mathbf{Q}]$ nennen wir *Ganzheitsbasis von K*, wenn $v_1,...,v_n$ den Ring der ganzen Zahlen von K als $\mathbf{Z}$-Modul erzeugt. Die Basis $1,\xi,\xi^2,...,\xi^{p-2}$ ist eine Ganzheitsbasis von $\mathbf{Q}(\xi)$.

Satz 3.6. *Für alle Zahlkörper K existiert eine Ganzheitsbasis.*

Beweis. Sei A der Ring der ganzen Zahlen von K und sei $v_1,...,v_n \in A$ eine Basis von K, so dass $D(v_1,...,v_n)$ minimal ist. Gesetzt, es gäbe ein $\alpha = \lambda_1 v_1 + ... + \lambda_n v_n \in A$ mit $\lambda_1,...,\lambda_n \in \mathbf{Q}$ und $\lambda_1 \notin \mathbf{Z}$. Sei $r = \lambda_1 - \lfloor\lambda_1\rfloor$, wo $\lfloor x\rfloor = \max\{n\in\mathbf{Z} : n \le x\}$ für $x \in \mathbf{R}$ ist. Dann aber ist $\alpha - \lfloor\lambda_1\rfloor v_1, v_2, ..., v_n$ eine Basis von K, welche in A liegt und welche

$$D(\alpha - \lfloor\lambda_1\rfloor v_1, v_2, ..., v_n) = r^2 D(v_1,...,v_n) < D(v_1,...,v_n)$$

erfüllt, was der Minimalität von $D(v_1,...,v_n)$ widerspricht. □

Wir haben nun den Ring $\mathbf{Z}[\xi]$ in Beziehung zum Körper $\mathbf{Q}(\xi)$ gesetzt. Kehren wir zurück zur ursprünglichen Frage nach den Einheiten von $\mathbf{Z}[\xi]$. Solche sind freilich durch die p-ten Einheitswurzeln gegeben. Nebst den p-ten Einheitswurzeln sind weitere Einheitswurzeln in $\mathbf{Z}[\xi]$ auch durch die $2p$-ten Einheitswurzeln $-\xi^r$ gegeben. Wir zeigen nun, dass dies die einzigen Einheitswurzeln in $\mathbf{Q}(\xi)$ sind. Wir werden die in Abschnitt 2 eingeführte Notation $\xi_n := \exp\left(\frac{2\pi i}{n}\right)$ verwenden.

Ist $\xi_l \in \mathbf{Q}(\xi_p)$, dann folgt

$$p-1 = [\mathbf{Q}(\xi_p):\mathbf{Q}] = [\mathbf{Q}(\xi_p):\mathbf{Q}(\xi_l)][\mathbf{Q}(\xi_l):\mathbf{Q}] \ge [\mathbf{Q}(\xi_l):\mathbf{Q}] = \varphi(l)$$

und wegen dem folgenden Lemma kann $\mathbf{Q}(\xi_p)$ die Einheitswurzel ξ_l nur für endlich viele $l \geq 1$ enthalten:

Lemma 3.7. *Für jede positive ganze Zahl n gilt $\varphi(n) \geq \sqrt{\frac{n}{2}}$.*

Beweis. Es ist klar, dass $\varphi(1) = \varphi(2) = 1$ ist. Wir nehmen zuerst an, n sei ungerade oder durch 4 teilbar. Sei $n = p_1^{k_1} \cdots p_m^{k_m}$ die Primfaktorisierung von n. Es ist wohlbekannt, dass

$$\varphi(n) = \prod_{i=1}^{m} \varphi(p_i^{k_i}) = \prod_{i=1}^{m} p_i^{k_i - 1}(p_i - 1)$$

ist. Für $k_i > 1$ ist $(k_i - 1)\log(p_i) + \log(p_i - 1) \geq (k_i - 1)\log(p_i) \geq \frac{k_i}{2}\log(p_i)$ und also ist $p_i^{k_i-1}(p_i - 1) \geq \sqrt{p_i}$. Falls $k_i = 1$ ist, dann ist $(p_i - 1) \geq \sqrt{p_i}$ für alle ungeraden Primzahlen p_i; dies gilt offenbar für $p_i = 3$, und die lineare Funktion $x \mapsto x + 1$ wächst schneller als die Wurzelfunktion. Durch unsere Wahl von n kommt der Faktor 2 in der Primfaktorisierung gar nicht oder mehrmals vor. Also ist $\varphi(n) \geq \sqrt{n}$.

Gesetzt, n sei gerade, aber nicht durch 4 teilbar. Dann ist $n = 2\nu$ für ein ungerades $\nu \in \mathbf{Z}$. Also ist $\varphi(n) = \varphi(2)\varphi(\nu) = \varphi(\nu) \geq \sqrt{\nu} = \sqrt{\frac{n}{2}}$ und das Lemma folgt. □

Sei G die Gruppe der Einheitswurzeln in $\mathbf{Q}(\xi_p)$. Die Gruppe G ist endlich, da jede Einheitswurzel in $\mathbf{Q}(\xi_p)$ (oder allgemeiner: in $\mathbf{C}$) von der Form ξ_l^r mit $l \geq 1$ und $0 \leq r \leq l - 1$ ist und ξ_l für nur endlich viele l in G enthalten ist. Die Gruppe G wird erzeugt von ξ_m mit $m := |G|$. Da ξ_p in der von ξ_m erzeugten Gruppe liegt, ist $p \mid m$ und $\mathbf{Q}(\xi_m) \supset \mathbf{Q}(\xi_p)$. Umgekehrt ist $\mathbf{Q}(\xi_m) \subset \mathbf{Q}(\xi_p)$, da $\xi_m \in \mathbf{Q}(\xi_p)$ liegt per Definition von G. Also gilt $\varphi(m) = \varphi(p)$.

Sei $k \geq 1$ so, dass $m = p^k m'$ mit $\mathrm{ggT}(m', p) = 1$. Dann ist $p - 1 = \varphi(p) = \varphi(m) = \varphi(p^k)\varphi(m') = (p - 1)p^{k-1}\varphi(m')$. Also ist $k = 1$ und $\varphi\left(\frac{m}{p}\right) = 1$. Somit ist $\frac{m}{p} = 1, 2$. Aber $m = p$ kann nicht sein, da $-\xi_p$ eine primitive $2p$-te Einheitswurzel ist, die in $\mathbf{Q}(\xi_p)$ liegt. Wir halten fest:

Lemma 3.8. *Die Einheitswurzeln in $\mathbf{Q}(\xi_p)$ sind $\pm\xi_p^r$ mit $0 \leq r < p$.*

Satz 3.9. *Für jede Einheit u in $\mathbf{Z}[\xi]$ existiert ein $u_1 \in \mathbf{R}$ und ein $r \in \mathbf{Z}$, so dass $u = \xi^r u_1$ ist.*

Um diesen Satz zu beweisen, brauchen wir ein Lemma:

Lemma 3.10. *Sei f ein normiertes Polynom mit ganzzahligen Koeffizienten und so, dass jede Nullstelle von f in $\mathbf{C}$ auf dem Einheitskreis liegt. Dann ist jede Nullstelle von f eine Einheitswurzel.*

Beweis. Für f konstant ist die Aussage des Lemmas klar. Seien $\alpha_1, ..., \alpha_r$ die Nullstellen von $f = X^r + a_{r-1}X^{r-1} + ... + a_1X + a_0$. Als Nullstellen eines Polynoms mit ganzzahligen Koeffizienten sind diese algebraische ganze Zahlen im Zerfällungskörper K von f über $\mathbf{Q}$. Da die Koeffizienten a_i Polynome bestehend aus höchstens $\binom{r}{i}$ Termen in $\alpha_1, ..., \alpha_r$ sind, können wir $|a_i|$ durch $\binom{r}{i}$ von oben abschätzen. Es kann also nur endlich viele ganzzahlige Polynome vom Grad r geben, deren Nullstellen auf dem Einheitskreis liegen.

Betrachten wir jetzt das Polynom $h_k = \prod_{i=1}^{r}(X - \alpha_i^k)$ mit $k \geq 1$. Ein Element $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$ operiert auf h_k in folgender Weise:

$$^{\sigma}(h_k) = \prod_{i=1}^{r}(X - \sigma(\alpha_i^k)) = \prod_{i=1}^{r}(X - \sigma(\alpha_i)^k) = h_k$$

und da σ beliebig war, müssen die Koeffizienten von h_k rational sein. Die Koeffzienten von h_k sind jedoch auch algebraische ganze Zahlen, folglich hat h_k ganzzahlige Koeffizienten.

Es gibt demnach zwei ganze Zahlen $m > n \geq 0$, so dass $h_m = h_n$ ist. Wir können eine Permutation $\tau \in S_r$ finden, so dass $\alpha_{\tau(i)}^m = \alpha_i^n$ ist für alle $1 \leq i \leq n$. Dann ist auch $\alpha_{\tau^2(i)}^{m^2} = \alpha_{\tau(i)}^{mn} = \alpha_i^{n^2}$. Induktiv folgt $\alpha_i^{m^{r!}} = \alpha_{\tau^{r!}(i)}^{m^{r!}} = \alpha_i^{n^{r!}}$, also ist $\alpha_i^{m^{r!}-n^{r!}} = 1$ für alle i. □

Beweis von Satz 3.9. Sei u eine Einheit von $\mathbf{Z}[\xi]$. Dann ist auch das komplex Konjugierte $\overline{u} \in \mathbf{Z}[\xi]$, wie leicht einzusehen ist, wenn wir u in der ganzen Basis $\xi, \xi^2, ..., \xi^{p-1}$ darstellen. Also ist $\overline{u}$ ebenso eine Einheit und das Element $\overline{u}^{-1}u \in \mathbf{Z}[\xi]$ hat Absolutbetrag 1 in $\mathbf{C}$.

Sei f das Minimalpolynom von $\overline{u}^{-1}u$ über $\mathbf{Q}$. Nach Lemma 2.1 hat f ganzzahlige Koeffzienten und da die Konjugierten von $\overline{u}^{-1}u$ wegen $\sigma(\overline{u})^{-1}\sigma(u) = \overline{\sigma(u)^{-1}}\sigma(u)$ für alle $\sigma \in \mathrm{Gal}(\mathbf{Q}(\xi)/\mathbf{Q})$ ebenfalls auf dem Einheitskreis liegen, folgt aus Lemma 3.10, dass $\overline{u}^{-1}u$ eine Einheitswurzel ist. Die Einheitswurzeln in $\mathbf{Q}(\xi)$ sind durch Lemma 3.8 gegeben. Sei $r \in \mathbf{Z}$ so, dass $u = \pm\overline{u}\xi^r$ ist.

An dieser Stelle bemerken wir, dass jede p-te Potenz eines Elements $\alpha \in \mathbf{Z}[\xi]$ kongruent zu einer ganzen Zahl modulo p ist. Stellen wir nämlich α als $a_0 + a_1\xi + ... + a_{p-2}\xi^{p-2}$ mit $a_0, ..., a_{p-2} \in \mathbf{Z}$ dar, ergibt sich

$$\alpha^p = (a_0 + a_1\xi + ... + a_{p-2}\xi^{p-2})^p \equiv a_0^p + a_1^p\xi^p + a_2^p\xi^{2p} + ... + a_{p-2}^p\xi^{p(p-2)} \pmod{p}.$$

Dies beweist insbesondere, dass $u^p \equiv \overline{u}^p \pmod{p}$ ist. Wäre $u = -\overline{u}\xi^r$, so folgte $u^p = (-\xi^r\overline{u})^p \equiv -u^p \pmod{p}$ und damit $2u^p \in (1-\xi)^{p-1}$. Dies implizierte, dass $u \in (1-\xi)$ läge, da $2 \notin (1-\xi)$ ist. Dies aber ist ein Widerspruch, weil wir u als Einheit gewählt haben.

Es ist also $u = \overline{u}\xi^r$. Wir setzen $u_1 := u\xi^{-r_1}$, wobei $r_1 \in \mathbf{Z}$ so gewählt sein soll, dass $2r_1 \equiv r \pmod{p}$ ist. Dann ist

$$\overline{u_1} = \xi^{r_1}\overline{u} = \xi^{r_1-r}u = \xi^{-r_1}u = u_1$$

und Satz 3.9 bewiesen. □

4. Die Klassenzahl

Sei in diesem Abschnitt K stets ein Zahlkörper und A stets dessen Ring der ganzen Zahlen.

Die *Idealnorm* N auf der Menge der Ideale von A sei definiert als die multiplikative Funktion mit $N(0) := 0$ und $N(\mathfrak{p}) := |A/\mathfrak{p}|$ für ein Primideal $\mathfrak{p}$. Der Ring $A/\mathfrak{p}$ ist endlich, da $A/\mathfrak{p}$ ein endlich-dimensionaler $\mathbf{Z}/p\mathbf{Z}$-Vektorraum ist mit $p\mathbf{Z} = \mathfrak{p} \cap \mathbf{Z}$ (siehe z.B. Satz 3.2); genauer gesagt, ist $p^{\dim_{\mathbf{Z}/p\mathbf{Z}}(A/\mathfrak{p})} = |A/\mathfrak{p}|$.

Die Funktion N ist wohldefiniert, da jedes Ideal $\mathfrak{a} \neq 0$ in A eine eindeutige Primfaktorisierung hat. Wir können $N(\mathfrak{a})$ auch als die Mächtigkeit des Ringes $A/\mathfrak{a}$ definieren. Für die Primfaktorisierung $\mathfrak{a} = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r}$ mit $r \geq 1$ und $k_1, ..., k_r \geq 1$ gilt nach dem Chinesischen Restsatz

$$A/\mathfrak{a} \cong \prod_{i=1}^{r} A/\mathfrak{p}_i^{k_i}.$$

Wie wir im Beweis von Satz 3.2 gesehen haben, ist $\dim_{\mathbf{Z}/p\mathbf{Z}}(A/\mathfrak{p}^k) = k \cdot \dim_{\mathbf{Z}/p\mathbf{Z}}(A/\mathfrak{p})$ und damit

$$|A/\mathfrak{a}| = \prod_{i=1}^{r} \left|A/\mathfrak{p}_i^{k_i}\right| = \prod_{i=1}^{r} p_i^{\dim_{\mathbf{Z}/p\mathbf{Z}}\left(A/\mathfrak{p}_i^{k_i}\right)} = \prod_{i=1}^{r} |A/\mathfrak{p}_i|^{k_i}$$

mit $p_i \in \mathbf{Z}$ so gewählt, dass $p_i\mathbf{Z} = \mathfrak{p}_i \cap \mathbf{Z}$ ist.

Seien p eine Primzahl und $\mathfrak{p}$ ein Primideal in A, so dass $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$ ist. Dann muss $\mathfrak{p}$ in der Primfaktorisierung von $p\mathbf{Z}$ vorkommen, ansonsten wäre $pA = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r} = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r} \cap \mathfrak{p} = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r}\mathfrak{p}$, was der Eindeutigkeit der Primfaktorisierung widerspräche. Es kann also nur endlich viele Primideale $\mathfrak{p}$ geben, so dass $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$ ist. Aber mehr noch: es kann nur endlich viele Primideale $\mathfrak{p}$ geben, so dass $N(\mathfrak{p})$ von p geteilt wird, da $N(\mathfrak{p})$ von p genau dann geteilt wird, wenn $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$ ist. Also gibt es für eine gegebene positive ganze Zahl n nur endlich viele Ideale $\mathfrak{a}$ in A, so dass $N(\mathfrak{a}) = n$ ist.

Die Idealnorm ist in gewissem Sinne eine Analogon der Körpernorm $N_{K/\mathbf{Q}}$:

Satz 4.1. *Sei $\alpha \in A$. Dann ist $\left|N_{K/\mathbf{Q}}(\alpha)\right| = N(\alpha A)$.*

Beweis. Der Ring A ist ein freier $\mathbf{Z}$-Modul vom Rang $n := [K : \mathbf{Q}]$. Das Bild unter der $\mathbf{Z}$-linearen Abbildung $A \to A, x \mapsto \alpha x$ ist ein $\mathbf{Z}$-Untermodul von A. Nach dem Elementarteilersatz [6, Ch. III, Thm. 7.8] ist $\mathrm{Im}(x \to \alpha x)$ ein freier $\mathbf{Z}$-Modul vom Rang n und wir können wir eine $\mathbf{Z}$-Basis $y_1, ..., y_n$ von A und Elemente $a_1, ..., a_n \in \mathbf{Z}$ so wählen, dass $a_1y_1, ..., a_ny_n$ eine $\mathbf{Z}$-Basis von $\mathrm{Im}(x \to \alpha x)$ ist. Die Diagonalmatrix $\mathrm{diag}(a_1, ..., a_n)$ ist die Abbildungsmatrix von $x \to \alpha x$ in bezug auf die Basis $y_1, ..., y_n$. $x \to \alpha x$ Es folgt $|\mathrm{coker}(x \mapsto \alpha x)| = |\mathbf{Z}/a_1\mathbf{Z} \times \cdots \times \mathbf{Z}/a_n\mathbf{Z}|$. Ferner ist

$$|\det(\mathrm{diag}(a_1, ..., a_n))| = a_1 \cdots a_n = |\mathrm{coker}(x \mapsto \alpha x)|$$

und somit ist $N(\alpha A) = |\mathrm{coker}(x \mapsto \alpha x)| = \left|N_{K/\mathbf{Q}}(\alpha)\right|$, was zu beweisen war. □

Wenn $\mathfrak{a}$ kein Hauptideal ist, so können wir trotzdem die Idealnorm in Beziehung zur Körpernorm setzen:

Satz 4.2. *Es existiert ein $C > 0$, so dass für alle Ideale $\mathfrak{a}$ in A ein $\alpha \in \mathfrak{a}$ existiert mit*

$$\left|N_{K/\mathbf{Q}}(\alpha)\right| \leq C \cdot N(\mathfrak{a}).$$

Beweis. Sei $n := [K : \mathbf{Q}]$ und $v_1, ..., v_n$ eine Ganzheitsbasis von K. Sei $\mathfrak{a}$ ein Ideal in A. Sei $m := \left\lfloor N(\mathfrak{a})^{\frac{1}{n}} \right\rfloor$.

Die Menge $S := \{k_1'v_1 + ... + k_n'v_n : 0 \leq k_i' \leq m, k_i' \in \mathbf{Z}\}$ hat Kardinalität $(m+1)^n > N(\mathfrak{a}) = |A/\mathfrak{a}|$. Es muss also zwei Elemente in S geben, deren Differenz in $\mathfrak{a}$ liegt; also existiert ein $\alpha = k_1v_1 + ... + k_nv_n \in \mathfrak{a}$ mit $k_i \in \mathbf{Z}$ und $|k_i| \leq m$. Also ist

$$\left|N_{K/\mathbf{Q}}(\alpha)\right| = \prod_\sigma |\sigma(\alpha)| \leq \prod_\sigma \left(\sum_i |k_i| \cdot |\sigma(v_i)|\right) \leq \prod_\sigma \left(\sum_i m \cdot |\sigma(\alpha)|\right) = m^n C,$$

wobei $C = \prod_\sigma \left(\sum_{i=1}^n |\sigma(v_i)|\right)$ ist und σ die $\mathbf{Q}$-Einbettungen von K in $\mathbf{C}$ sind. Aus der Definition von m folgt, dass $\left|N_{K/\mathbf{Q}}(\alpha)\right| \leq C \cdot N(\mathfrak{a})$ ist. Die Konstante C ist positiv, da jedes σ eine injektive Abbildung ist. □

Uns interessiert im weiteren nicht, wie die Konstante C aussieht. Ein Satz von Minkowski gibt eine explizite Konstante: Sei $2s$ die Anzahl der Paare nicht-reeller Einbettungen eines Zahlkörpers K und D die Diskriminante einer Ganzheitsbasis von K (welche, wie im Beweis zu Satz 3.6 gezeigt, invariant unter der Wahl einer Ganzheitsbasis ist). Dann erfüllt $C = \left(\frac{2}{\pi}\right)^s \sqrt{D}$ die Bedingung von Satz 4.2. Genaueres kann beispielsweise in [5] nachgelesen werden.

Die in Abschnitt 2 eingeführte Klassengruppe H_K ist trivial, falls A ein Hauptidealring ist, da, wie wir gesehen haben, in jeder Nebenklasse von H_K ein Ideal von A enthalten ist. Im Allgemeinen muss A kein Hauptidealring sein, doch die Klassengruppe wird noch immer endlich sein. Mit dem eben gezeigten Satz lässt sich dies folgendermassen beweisen:

Sei $\Xi \in H_K$ und sei $\mathfrak{a}$ ein Ideal in A, das in Ξ^{-1} liegt. Sei $\alpha \in \mathfrak{a}$ wie in Satz 4.2 und sei $\mathfrak{b}$ ein Ideal in A, so dass $\mathfrak{ab} = (\alpha)$ ist. Dann gilt:

$$N(\mathfrak{a})N(\mathfrak{b}) = N(\mathfrak{ab}) = \left|N_{K/\mathbf{Q}}(\alpha)\right| \leq C \cdot N(\mathfrak{a}).$$

Somit existiert für jedes $\Xi \in H_K$ ein Ideal $\mathfrak{b} \in \Xi$ mit der Eigenschaft $N(\mathfrak{b}) \leq C$. Da es für jede positive ganze Zahl n nur endlich viele Ideale geben kann, deren Idealnorm gleich n ist, existieren nur endlich viele Nebenklassen.

Definition 4.3. Die *Klassenzahl* h_K eines Zahlkörpers K ist definiert als die Ordnung der Klassengruppe H_K.

Der Ring A ist also ein Hauptidealring genau dann, wenn die Klassenzahl von K gleich 1 ist. Die Aussage lässt sich mit dem folgendem Satz verallgemeinern.

Satz 4.4. *Ein Dedekindring ist faktoriell genau dann, wenn er ein Hauptidealring ist.*

Beweis. Jeder Hauptidealring ist faktoriell [6, Ch. 2, Thm. 5.2].

Wir nehmen an, dass A Dedekind und faktoriell ist. Sei $\mathfrak{a} \neq 0$ ein Ideal in A und sei $a \in \mathfrak{a}$ nicht Null. Wir können $a = up_1 \cdots p_n$, $n > 1$, als eindeutiges Produkt von irreduziblen Elementen p_i und einer Einheit u schreiben (eindeutig bis auf Umordnung und Multiplikation mit einer Einheit).

Jedes Ideal $\mathfrak{a}$ in einem Dedekindring kann als eindeutiges Produkt von Primidealen geschrieben werden; sei also $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_m$ für Primideale $\mathfrak{p}_i$. Wir erhalten $(a) = (p_1) \cdots (p_n) \subset \mathfrak{p}_1 \cdots \mathfrak{p}_m = \mathfrak{a}$. Die Ideale $(p_1), ..., (p_n)$ sind prim und jedes Ideal, das im Ideal $\mathfrak{a}$ enthalten ist, teilt dieses auch. Mithin müssen die Ideale $\mathfrak{p}_i$ von der Form (p_j) sein und sind Hauptideale. Also ist auch $\mathfrak{a}$ ein Hauptideal. □

Korollar 4.5. *Der Ring der ganzen Zahlen eines Zahlkörpers K ist faktoriell genau dann, wenn $h_K = 1$ ist.*

Sei p eine Primzahl. Um die Notation etwas einfacher zu gestalten, werden wir für die Klassenzahl von $\mathbf{Q}(\xi_p)$ anstatt $h_{\mathbf{Q}(\xi_p)}$ stets h_p schreiben. Die zu Beginn des dritten Abschnittes erwähnte Idee, die Gleichung $x^p + y^p = z^p$ als $z^p = (x+y)(x+\xi_p y)(x+\xi_p^2 y) \cdots (x+\xi_p^{p-1} y)$ mit $x, y, z \in \mathbf{Z}[\xi_p]$ zu schreiben, lässt uns auf einen Beweis für die Exponenten p mit $h_p = 1$ hoffen. Dies gibt uns allerdings nur wenige Resultate, wie der folgende Satz zeigt:

Satz 4.6 (Uchida)**.** *Sei p eine Primzahl. Es ist $h_p = 1$ genau dann, wenn $p \leq 19$ ist.*

Der Beweis ist in [7] nachzulesen. Darin wird zuerst mithilfe des Brauer-Siegel-Theorems eine obere Schranke für die Primzahlen p mit $h_p = 1$ berechnet, danach mithilfe eines Computers der explizite Wert 19 gefunden.

Also müssen wir eine schwächere Bedingung für den Exponenten p finden, so dass wir noch immer mit der Gleichung $z^p = (x+y)(x+\xi_p y)(x+\xi_p^2) \cdots (x+\xi_p^{p-1} y)$ arbeiten können, aber der Ring $\mathbf{Z}[\xi_p]$ nicht mehr zwingend faktoriell sein muss. Diese wird für uns die folgende sein:

Definition 4.7. Eine Primzahl p heisse regulär, wenn p die Klassenzahl h_p nicht teilt.

Die Klassengruppe $H_{\mathbf{Q}(\xi_p)}$ für eine reguläre Primzahl p hat trivialen p-Torsionsanteil.

5. Adele und Idele

Dieser Abschnitt dient der Erarbeitung des Vokabulars, um die Sätze aus der Klassenkörpertheorie in Abschnitt 6 zu verstehen. Dazu verallgemeineren wir den Begriff des Absolutbetrags:

Definition 5.1. Ein *Absolutbetrag* auf einem Körper K ist eine Funktion

$$|\cdot| : \begin{cases} K & \to & [0,\infty) \\ x & \mapsto & |x| \end{cases},$$

so dass für alle $x, y \in K$ gilt:

(1) $|x| = 0 \Leftrightarrow x = 0$
(2) $|x \cdot y| = |x| \cdot |y|$
(3) $|x + y| \leq |x| + |y|$.

Abgesehen vom Beweis von Satz 5.11 werden wir Absolutbeträge stets auf Zahlkörpern betrachten. Jeder Absolutbetrag $|\cdot|$ induziert eine Metrik $d(x, y) := |x - y|$, wie einfach nachgeprüft werden kann. Die Topologie, die durch diese Metrik auf K erzeugt wird, nennen wir die von $|\cdot|$ erzeugte Topologie. Zwei Absolutbeträge $|\cdot|$ und $|\cdot|'$ nennen wir äquivalent und schreiben $|\cdot| \sim |\cdot|'$, wenn sie dieselbe Topologie erzeugen. Es ist klar, dass dies eine Äquivalenzrelation ist.

Den Absolutbetrag, der durch $|x| := 1$ für alle $x \neq 0$ definiert ist, nennen wir den *trivialen Absolutbetrag* und werden wir stets aus unseren Betrachtungen ausschliessen.

Das klassische Beispiel eines Absolutbetrages ist die Funktion $|\cdot|_\infty$ auf $\mathbf{Q}$, gegeben durch $|x|_\infty := x$ für $x \geq 0$ und $|x|_\infty = -x$ für $x < 0$. Die metrische Vervollständigung bezüglich der von $|\cdot|_\infty$ induzierten Metrik sind die reellen Zahlen. Allgemein kann die metrische Vervollständigung bezüglich eines Absolutbetrages $|\cdot|$ auf einem Körper K mit einer natürlichen Körperstruktur versehen werden.

Der Absolutbetrag $|\cdot|_\infty$ ist nicht das einzige Beispiel eines Absolutbetrages auf $\mathbf{Q}$. Wir definieren die p-adische Bewertung einer ganzen Zahl $x \neq 0$ als $\mathrm{ord}_p(x) := \max\{a \in \mathbf{Z}_{\geq 0} : p^a \mid x\}$. Die p-adische Bewertung von 0 sei $+\infty$. Die p-adische Bewertung einer rationalen Zahl $\frac{y}{z}$ mit teilerfremden $y, z \in \mathbf{Z}$ sei definiert als $\mathrm{ord}_p\left(\frac{y}{z}\right) := \mathrm{ord}_p(y) - \mathrm{ord}_p(z)$. Der *$p$-adische Absolutbetrag* sei dann $|x|_p := \frac{1}{p^{\mathrm{ord}_p(x)}}$. Die Vervollständigung von $\mathbf{Q}$ bezüglich der von $|\cdot|_p$ induzierten Metrik ist der Ring der p-adischen Zahlen $\mathbf{Q}_p$. Von nun an werden wir schlicht „Vervollständigung bezüglich eines Absolutbetrags“ sagen, wenn wir die Vervollständigung bezüglich der vom Absolutbetrag induzierten Metrik meinen.

Es gibt einen bedeutenden Unterschied zwischen $|\cdot|_\infty$ und $|\cdot|_p$. Für alle ganzen Zahlen n ist nämlich $|n|_p \leq 1$, was freilich nicht der Fall ist für $|\cdot|_\infty$. Einen Absolutbetrag $|\cdot|$ nennen wir *nicht-archimedisch*, falls $|n| \leq 1$ ist für alle $n \in \mathbf{Z}$ und ansonsten *archimedisch*.

Proposition 5.2. *Ein Absolutbetrag ist genau dann nicht-archimedisch, wenn $|x+y| \leq \max\{|x|, |y|\}$ ist für alle $x, y \in K$.*

Beweis. Wir zeigen, dass jeder Absolutbetrag $|\cdot|$, so dass die Funktion $\mathbf{Z} \to [0,\infty)$, $n \mapsto |n|$ beschränkt ist, nicht-archimedisch ist. Man nehme an, dass eine obere Schranke gegeben sei durch $C > 0$ (wir

könnten auch $C \geq 1$ annehmen, da für jeden Absolutbetrag $|1| = 1$ ist). Dann ist

$$\begin{aligned} |x+y|^n &= \left| \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \right| \\ &\leq \sum_{k=0}^{n} \left| \binom{n}{k} \right| |x|^{n-k} |y|^k \\ &\leq C \sum_{k=0}^{n} |x|^{n-k} |y|^k \leq C \cdot n \cdot \max\{|x|, |y|\}^n \end{aligned}$$

und wenn wir auf beiden Seiten die n-te Wurzel ziehen, erhalten wir

$$|x+y| \leq \sqrt[n]{n}\, \sqrt[n]{C} \max\{|x|, |y|\} \to \max\{|x|, |y|\}, \text{ wenn } n \to +\infty.$$

Also induziert jeder nicht-archimedische Absolutbetrag eine Ultrametrik. Für die Umkehrung sei $|\cdot|'$ archimedisch und sei n_0 die kleinste positive ganze Zahl, so dass $|n_0|' > 1$ ist. Dann ist $|n_0|' > \max\{|1|, |n_0 - 1|\} = 1$. □

Satz 5.3. *Zwei Absolutbeträge $|\cdot|$ und $|\cdot|'$ auf einem Zahlkörper K sind äquivalent genau dann, wenn ein $e > 0$ existiert, so dass $|\cdot|^e = |\cdot|'$.*

Beweis. Es ist klar, dass zwei Absolutbeträge $|\cdot|$ und $|\cdot|'$ mit $|\cdot|^e = |\cdot|'$ dieselbe Topologie erzeugen. Die Umkehrung folgt aus dem folgenden Lemma und der Tatsache, dass $|ab^{-1}| < 1$ ist für $a, b \in K$ genau dann, wenn $(ab^{-1})^n$, $n \in \mathbf{N}$, eine Nullfolge ist und damit $|ab^{-1}| < 1$ ist genau dann, wenn $|ab^{-1}|' < 1$ ist. Der Satz folgt dann aus dem nachfolgenden Lemma. □

Lemma 5.4. *Gegeben zwei Absolutbeträge $|\cdot|$ und $|\cdot|'$ auf einem Zahlkörper K, so dass $|a| < |b| \Rightarrow |a|' < |b|'$ für alle $a, b \in K$. Dann existiert ein $e > 0$, so dass $|\cdot|^e = |\cdot|'$.*

Beweis. Sei $y \in K$ so, dass $|y| > 1$ ist. Ein solches Element muss existieren, da ansonsten der Absolutbetrag trivial ist – schliesslich impliziert $|x| < 1$, dass $|x^{-1}| > 1$ ist. Für ein beliebiges Element $x \in K^\times$ existiert ein $c \in \mathbf{R}$, so dass $|x| = |y|^c$. Man wähle eine von oben nach c konvergierende Folge $\left(\frac{a_n}{b_n}\right)_{n \in \mathbf{N}}$ mit $a_n, b_n \in \mathbf{Z}$. Dann gilt $|x| = |y|^c < |y|^{\frac{a_n}{b_n}}$ und demnach ist $|x^{b_n}| < |y^{a_n}|$.

Nach Voraussetzung ist $|x^{b_n}|' < |y^{a_n}|'$ für alle $n \in \mathbf{N}$, woraus $|x|' \leq |y|'^c$ folgt. Dasselbe Argument mit einer von unten nach c konvergierenden Folge ist gibt $|x|' \geq |y|'^c$. Also ist

$$\frac{\log |x|}{\log |x|'} = \frac{\log |y|}{\log |y|'}.$$

Da x beliebig war, muss $|\cdot|^e = |\cdot|'$ mit $e := \frac{\log |y|'}{\log |y|}$ sein. □

Aus Satz 5.3 folgt auch, dass ein archimedischer Absolutbetrag $|\cdot|$ einzig zu einem archimedischen Absolutbetrag $|\cdot|'$ äquivalent sein kann, denn ansonsten wäre die rechte Seite der Gleichung $|n|^e = |n|'$ mit $n \in \mathbf{Z}$ für $n \to +\infty$ beschränkt, während sie auf der linken Seite unbeschränkt wäre.

Für archimedische Absolutbeträge gilt der folgende Satz:

Satz 5.5. *Der einzige archimedische Absolutbetrag auf $\mathbf{Q}$ bis auf Äquivalenz ist $|\cdot|_\infty$.*

Wir verzichten hier auf den Beweis, da wir uns im folgenden hauptsächlich mit nicht-archimedischen Absolutbeträgen beschäftigen werden. Nachzulesen ist der Beweis z.B. in [11, Ch. 2.3].

Die sich ergebende Frage ist, ob es eine ähnliche Charakterisierung der nicht-archimedischen Absolutbeträge auf $\mathbf{Q}$ gäbe. Um diese Frage zu beantworten, definieren wir zuerst den *Bewertungsring* eines nicht-archimedischen Absolutbetrags $|\cdot|$ auf einem Zahlkörper K, welcher der Unterring $\mathcal{O} := \{x \in K : |x| \leq 1\}$ sein soll.

Da $|x + y| \leq \max\{|x|, |y|\}$ ist, ist $\mathcal{O}$ abgeschlossen unter Addition. Der Ring $\mathcal{O}$ ist ein lokaler Ring mit maximalem Ideal $\mathfrak{m} = \{x \in \mathcal{O} : |x| < 1\}$.

Satz 5.6. *Sei K ein Zahlkörper und A dessen Ring der ganzen Zahlen. Dann ist $A = \bigcap_{|\cdot|} \mathcal{O}_{|\cdot|}$, wobei der Schnitt über alle nicht-archimedischen Absolutbeträge $|\cdot|$ auf K geht und $\mathcal{O}_{|\cdot|}$ deren Bewertungsring bezeichnet.*

Wir zeigen einzig die Richtung, die wir brauchen werden: Sei $x \in A$ und seien $a_0, ..., a_{n-1} \in \mathbf{Z}$ so, dass $x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0$ ist. Sei $|\cdot|$ ein nicht-archimedischer Absolutbetrag. Dann ist $|x|^n \leq \max\{1, |x|, ..., |x|^{n-1}\}$. Doch wenn $|x| \geq 1$ ist, dann folgt, dass $|x|^n \geq |x|^{n-1}$ ist, und somit ist $|x| = 1$. Die andere Richtung des Beweises kann in [8, Ch. 10, Thm. 3.1] nachgelesen werden.

Lemma 5.7. *Seien $|\cdot|$ und $|\cdot|'$ zwei nicht-archimedische Absolutbeträge auf einem Zahlkörper K und seien $\mathcal{O}$, $\mathcal{O}'$ deren Bewertungsringe. Es ist $\mathcal{O} = \mathcal{O}'$ genau dann, wenn $|\cdot|$ zu $|\cdot|'$ äquivalent ist.*

Beweis. Wenn die Absolutbeträge äquivalent sind, folgt aus Satz 5.3, dass $\mathcal{O} = \mathcal{O}'$ ist. Aus Lemma 5.4. folgt, dass $\mathcal{O} \subset \mathcal{O}'$ impliziert, dass $|\cdot|$ äquivalent zu $|\cdot|'$ ist. □

Satz 5.8. *Die einzigen nicht-archimedischen Absolutbeträge auf $\mathbf{Q}$ sind bis auf Äquivalenz $|\cdot|_p$ für Primzahlen p.*

Beweis. Sei $|\cdot|$ ein nicht-archimedischer Absolutbetrag. Der Bewertungsring $\mathcal{O}$ von $|\cdot|$ enthält als Unterring von $\mathbf{Q}$ den Ring $\mathbf{Z}$. Sei $\mathfrak{m}$ das maximale Ideal in $\mathcal{O}$ und p eine Primzahl, so dass $p\mathbf{Z} = \mathfrak{m} \cap \mathbf{Z}$ ist. Eine solche Primzahl existiert, da $|\cdot|$ nicht-trivial ist: Denn $\mathfrak{m} \cap \mathbf{Z}$ ist ein Primideal als Urbild der Inklusion $\mathbf{Z} \to \mathcal{O}$ und $(0) = \mathfrak{m} \cap \mathbf{Z}$ gilt genau dann, wenn $|n| = 1$ für alle $n \in \mathbf{Z} - \{0\}$ gilt. Dies aber wiederum heisst, dass für jede rationale Zahl $\frac{x}{y}$ mit $x, y \in \mathbf{Z} - \{0\}$ auch $\left|\frac{x}{y}\right| = 1$ gilt und $|\cdot|$ trivial ist.

Wegen der Lemmata 5.3 und 5.7 brauchen wir nur zu zeigen, dass der Bewertungsring $\mathcal{O}_p$ von $|\cdot|_p$ in $\mathcal{O}$ enthalten ist. Gesetzt, $x \in \mathbf{Q}$ sei nicht in $\mathcal{O}$ enthalten. Dann ist $nx \in \mathbf{Z} \subset \mathcal{O}$ für eine kleinste positive ganze Zahl n. Es ist $nxx^{-1} \in \mathfrak{m}$, also liegt n in $\mathfrak{m}$. Wegen der Definiton der Primzahl p teilt diese n. Aufgrund der Minimalität von n ist $\mathrm{ord}_p(x) < 0$. Demzufolge ist $\mathcal{O}_p \subset \mathcal{O}$. □

Für zwei Primzahlen $p \neq q$ sind die Absolutbeträge $|\cdot|_p$ und $|\cdot|_q$ nicht äquivalent, da $|p|_p < 1$ ist, aber $|p|_q = 1$. Zusammen mit Satz 5.4 gibt der vorherige Satz:

Satz 5.9 (Ostrowski)**.** *Die einzigen Absolutbeträge auf $\mathbf{Q}$ sind bis auf Äquivalenz $|\cdot|_p$ für Primzahlen p und $|\cdot|_\infty$.*

Korollar 5.10. *Für ein gegebenes $a \in \mathbf{Q}$ existieren nur endlich viele nicht-äquivalente Absolutbeträge $|\cdot|$ auf $\mathbf{Q}$, so dass $|a| > 1$ ist.*

Beweis. Sei $a = \frac{b}{c}$ mit $b, c \in \mathbf{Z}$ koprim. Es ist $\left|\frac{b}{c}\right|_p > 1$ genau dann, wenn b von p geteilt wird. Es kann aber nur endlich viele Primzahlen geben, die b teilen. □

Wir haben nun einiges zu Absolutbeträgen auf $\mathbf{Q}$ gesehen. Unser Ziel ist im weiteren das eben gezeigte Korollar auf allgemeine Zahlkörper zu verallgemeinern. Dazu benötigen wir zuerst ein Lemma:

Lemma 5.11. *Sei p eine Primzahl. Der Körper der p-adischen Zahlen $\mathbf{Q}_p$ sind lokalkompakt. Insbesondere ist der Einheitsball eines endlich-dimensionalen Vektorraumes über $\mathbf{Q}_p$ kompakt.*

Wir verzichten auf den Beweis, da dieser zu weit von der eigentlichen Aufgabe wegführt. Der Beweis des Satzes ist in [10, Cor. 3.3.8] zu finden.

Uns interessieren die Erweiterungen eines Absolutbetrags $|\cdot|$ von $\mathbf{Q}$ auf einen Zahlkörper K. Darunter verstehen wir einen Absolutbetrag $|\cdot|'$ auf K, so dass dessen Einschränkung auf $\mathbf{Q}$ gleich $|\cdot|$ ist.

Satz 5.12. *Für einen Zahlkörper K vom Grad n und einen Absolutbetrag $|\cdot|$ auf $\mathbf{Q}$ existieren höchstens n Erweiterungen von $|\cdot|$ auf K.*

Beweis. Nach dem Satz vom primitiven Element [6, Ch. V, Thm 4.6] existiert ein $\gamma \in K$, so dass $K = \mathbf{Q}(\gamma)$ ist. Sei f das Minimalpolynom von γ über $\mathbf{Q}$. Der Grad von f ist genau $n := [K : \mathbf{Q}]$.

Sei L die Vervollständigung von $\mathbf{Q}$ bezüglich $|\cdot|$. Als Polynom in $L[X]$ ist f nicht unbedingt irreduzibel. Schreiben wir also $f = \prod_{j=1}^{J} g_j$ als Produkt von irreduziblen Faktoren $g_j \in L[X]$. Sei $L_j = L(\beta_j)$ mit β_j einer Nullstelle von g_j. Sei $L \otimes_{\mathbf{Q}} K$ das Tensorprodukt von $\mathbf{Q}$-Algebren. Wir können einen $\mathbf{Q}$-Algebra-Homomorphismus $\mu_j : L \otimes_{\mathbf{Q}} K \to L_j$ via $a \otimes \gamma^k \mapsto a\beta_j^k$ und ferner eine Komposition κ von $\mathbf{Q}$-Algebra-Homomorphismen

$$K \to L \otimes_{\mathbf{Q}} K \to \bigoplus_{j=1}^{J} L_j$$

definieren. Da κ ein Ringhomomorphismus und $\bigoplus_{j=1}^{J} L_j \neq 0$ ist, folgt, da K ein Körper ist, dass κ injektiv ist.

Für $a \in L_j$ sei $|a|_j := \left|N_{L_j/L}(a)\right|^{\frac{1}{n_j}}$ mit $n_j := [L_j : L]$. Die Einschränkung von $|\cdot|_j$ auf K ist $|\cdot|$. Klarerweise gilt $|a|_j \geq 0$ und $|ab|_j = |a|_j|b|_j$ für alle $a, b \in L_j$. Wir zeigen, dass für $|\cdot|_j$ die Dreiecksungleichung gilt.

Sei $\|\cdot\|_j$ eine Maximum-Norm auf dem L-Vektorraum L_j, d.h. für eine feste Basis $b_1, ..., b_{n_j}$ von L_j und $a = \lambda_1 b_1 + ... + \lambda_{n_j} b_{n_j}$ mit $\lambda_1, ..., \lambda_{n_j} \in L$ sei $\|a\|_j := \max\{|\lambda_i| : 1 \leq i \leq n_j\}$. Der Einheitsball $S := \{x \in L_j : \|x\|_j = 1\}$ ist kompakt, da L entweder gleich $\mathbf{Q}_p$ oder $\mathbf{R}$ ist.

Die Abbildung $|\cdot|_j$ ist stetig auf L_j. Wegen der Kompaktheit von S existieren $C_1, C_2 > 0$, so dass $C_1 < |a| < C_2$ für alle $a \in S$ gilt.

Sei $a = \lambda_1 b_1 + ... + \lambda_{n_j} b_{n_j} \neq 0$ und sei λ der grösste der Koeffizienten λ_j in Bezug auf $|\cdot|$. Dann ist

$$C_1 \leq \frac{\left|\frac{a}{\lambda}\right|_j}{\left\|\frac{a}{\lambda}\right\|_j} \leq C_2$$

und also

$$C_1 \leq \frac{|a|_j}{\|a\|_j} \leq C_2.$$

Wir können annehmen, dass $C_1 = C_2^{-1}$ ist, andernfalls vergrössern wir C_2 oder verkleinern C_1. Wir erhalten für alle $a, b \in L_j$:

$$|a+b|_j \leq C_2 \cdot (\|a+b\|_j) \leq C_2 \cdot (\|a\|_j + \|b\|_j) \leq C_1 C_2 \cdot (|a|_j + |b|_j) = |a|_j + |b|_j.$$

Es ist gezeigt, dass $|\cdot|_j$ ein Absolutbetrag auf L_j ist. Da K in $\bigoplus_{j=1}^J L_j$ eingebettet werden kann, definieren wir $|a|_j^* := |\kappa_j(a)|_j$ für $a \in K$, wobei κ_j die von κ induzierte injektive lineare Abbildung $K \to L_j$ sei. Per Konstruktion ist $|\cdot|_j^*$ auf K ein Absolutbetrag.

Wir zeigen, dass jede Erweiterung $|\cdot|'$ von $|\cdot|$ auf K äquivalent zu $|\cdot|_j^*$ sein muss für ein $1 \leq j \leq J$. Zuerst merken wir an, dass $|\cdot|_j^*$ eine Norm auf L_j als L-Vektorraum induziert.

Wir definieren nun auf $L \otimes_{\mathbf{Q}} K$ die folgende Topologie: Sei $v_1, ..., v_n$ eine Basis von K. Jedes Element von $L \otimes_{\mathbf{Q}} K$ kann eindeutig in der Form $\sum_{i=1}^n a_i \otimes_{\mathbf{Q}} v_i$ geschrieben werden. Somit sind die Mengen $L \otimes_{\mathbf{Q}} K$ und L^n bijektiv. Die Topologie auf $L \otimes_{\mathbf{Q}} K$ sei gegeben durch die Produkttopologie auf L^n. Es ist nicht schwierig zu zeigen, dass diese Definition nicht von der Wahl der Basis abhängt. Ferner ist $\mathbf{Q} \otimes_{\mathbf{Q}} K$ homöomorph zu $\mathbf{Q}^n \subset L^n$ und damit dicht in $L \otimes_{\mathbf{Q}} K$.

Ebenfalls ist

$$\dim_L (L \otimes_{\mathbf{Q}} K) = \dim_{\mathbf{Q}}(K) = \deg f = \sum_{j=1}^J \deg g_j = \dim_L \left(\bigoplus_{j=1}^J L_j \right)$$

und somit sind $L \otimes_{\mathbf{Q}} K$ und $\bigoplus_{j=1}^J L_j$ isomorph als topologische L-Vektorräume.

Da $\mathbf{Q} \otimes_{\mathbf{Q}} K$ ein dichter Unterraum von $L \otimes_{\mathbf{Q}} K$ ist, können wir $|\cdot|'$ stetig von $\mathbf{Q} \otimes_{\mathbf{Q}} K$ zu einer reellwertigen Funktion auf $L \otimes_{\mathbf{Q}} K$ erweitern und damit auch als reellwertige Funktion auf $\bigoplus_{j=1}^J L_j$ sehen. Die Funktion $|\cdot|'$ ist nicht mehr zwingend ein Absolutbetrag; wegen der Stetigkeit gilt zwar noch immer $|x+y|' \leq |x|' + |y|'$ und $|xy|' = |x|'|y|'$ für alle $x, y \in L \otimes_{\mathbf{Q}} K$, es muss jedoch nicht mehr zwingend $|x|' = 0 \Leftrightarrow x = 0$ gegeben sein.

Seien $a_1 \in L_{j_1}$ und $a_2 \in L_{j_2}$ so, dass $|a_1|'$ und $|a_2|'$ nicht Null sind. Falls $j_1 \neq j_2$ ist, dann führt $0 = |a_1 a_2|' = |a_1|'|a_2|' \neq 0$ zum Widerspruch. Also kann die Einschränkung von $|\cdot|'$ auf L_j für höchstens ein j nicht konstant Null sein. Allerdings kann $|\cdot|'$ nicht auf allen L_j konstant Null sein, da $L \otimes_{\mathbf{Q}} K$ nicht die triviale Topologie trägt. Es existiert also genau ein L_j, so dass die Einschränkung von $|\cdot|'$ auf L_j nicht Null ist.

Falls $a \neq 0$ in L_j liegt und $|a|' \neq 0$ ist, dann ist für $b \neq 0$ in L_j auch $0 \neq |a|' = |b|'|ab^{-1}|'$ und damit $|b|' \neq 0$. Die Einschränkung von $|\cdot|'$ auf L_j ist ein Absolutbetrag.

Der Beweis ist komplett, wenn wir gezeigt haben, dass $|\cdot|_j^*$ die einzige Erweiterung von $|\cdot|$ auf L_j ist, da K in L_j enthalten ist. Ein Absolutbetrag auf L_j ist jedoch eine Norm auf L_j und alle Normen auf L_j sind äquivalent zueinander und erzeugen dieselbe Topologie auf L_j, da L_j endlichdimensional ist (siehe z.B. [9, Thm. 1.2.6] für den Fall eines $\mathbf{R}$-Vektorraums; der Beweis für einen endlich-dimensionalen Vektorraum über einem lokalkompakten Körper ist analog). Also ist jede weitere Erweiterung auf L_j äquivalent zu $|\cdot|'$. □

Korollar 5.13. *Es gibt nur endlich viele nicht-äquivalente archimedische Absolutbeträge auf einem Zahlkörper K.*

Wir können nun Korollar 5.9 auf Zahlkörper verallgemeinern:

Satz 5.14. *Sei K ein Zahlkörper. Für ein gegebenes $a \in K$ existieren nur endliche viele nicht-äquivalente Absolutbetrage $|\cdot|$ auf K, so dass $|a| > 1$ ist.*

Beweis. Jedes Element $a \in K$ ist algebraisch; sei a Nullstelle des Polynoms $X^n+b_{n-1}X^{n-1}+...+b_1X+b_0$ mit $b_0, ..., b_{n-1} \in \mathbf{Q}$. Sei $|\cdot|$ ein nicht-archimedischer Absolutbetrag. Somit ist

$$|a|^n \leq \max\{|b_0|, |a| \cdot |b_1|, ..., |a|^{n-1}|b_{n-1}|\} \leq \max\{1, |a|^{n-1}\} \cdot \max\{|b_0|, ..., |b_{n-1}|\}$$

und somit

$$|a| \leq \max\{|b_0|, ..., |b_{n-1}|\}.$$

Die rechte Seite der Ungleichung ist beschränkt durch 1 für fast alle Absolutbetrage $|\cdot|$ auf $\mathbf{Q}$ (bis auf Äquivalenz) nach Korollar 5.9. Jeder der Absolutbetrage, für welche die rechte Seite nicht beschränkt ist, hat höchstens endlich viele Erweiterungen auf K nach Satz 5.11. Dies beweist den Satz. □

Lemma 5.15. *Sei K ein Zahlkörper vom Grad n und A dessen Ring der ganzen Zahlen. Sei $|\cdot|$ ein nicht-archimedischer Absolutbetrag auf $\mathbf{Q}$ und seien $|\cdot|_1, ..., |\cdot|_r$, $r \leq n$, ein vollständiger Satz nicht-äquivalenter Erweiterungen von $|\cdot|$ auf K. Dann sind die Primideale $\mathfrak{p}_i := \{x \in A : |x|_i < 1\}$ paarweise koprim.*

Beweisskizze. Dass $\mathfrak{p}_i$ für alle i ein Primideal ist, folgt aus Satz 5.6. Unter Verwendung von [1, Prop. 9.2, Prop. 9.3] ist leicht zu zeigen, dass der lokalisierte Ring $A_{\mathfrak{p}_i}$ ein Hauptidealring ist.

Sei π ein Element, welches das maximale Ideal von $A_{\mathfrak{p}_i}$ erzeugt und sei $\mathrm{ord}_\pi(x) := \max\{k \in \mathbf{Z} : \pi^k y = x, y \in A_{\mathfrak{p}_i}\}$ für $x \in A_{\mathfrak{p}_i}$. Der Körper K ist der Quotientenkörper von A, also *a fortiori* von $A_{\mathfrak{p}_i}$. Wenn wir den Beweis von Satz 5.7 imitieren, erhalten wir, dass $|\cdot|_i \sim |\cdot|_\pi$ ist.

Wäre $\mathfrak{p}_i = \mathfrak{p}_j$ für $j \neq i$, dann wäre $|\cdot|_j \sim |\cdot|_\pi \sim |\cdot|_i$ im Widerspruch zur Voraussetzung. □

Das Lemma 5.14 impliziert, dass $|\cdot|_p$ nur eine einzige Erweiterung auf $\mathbf{Q}(\xi_p)$ hat. Es beweist ferner Satz 5.11 im nicht-archimedischen Fall, da nach Satz 3.2 für eine Primzahl q höchstens n verschiedene Primideale von A über $q\mathbf{Z}$ liegen können.

Wir schreiben nun einfacher $\mathfrak{p}$ für eine Äquivalenzklasse von Absolutbeträgen auf einem Zahlkörper K und $K_\mathfrak{p}$ für die Vervollständigung bezüglich eines Absolutbetrages in $\mathfrak{p}$.

Der *Adelring* von K ist definiert als der Ring

$$\mathbf{A}_K := \left\{ (\alpha_\mathfrak{p}) \in \prod_\mathfrak{p} K_\mathfrak{p} : |\alpha_\mathfrak{p}|_\mathfrak{p} \leq 1 \text{ für fast alle } \alpha_\mathfrak{p} \right\}$$

wobei $|\cdot|_\mathfrak{p}$ ein Repräsentant der Äquivalenzklasse $\mathfrak{p}$ sei. Da offenbar $(1)_\mathfrak{p} \in \mathbf{A}_K$ liegt, ist $\mathbf{A}_K$ nicht-leer. Nach Satz 5.13 enthält $\mathbf{A}_K$ sogar K als Unterring.

Die Einheitengruppe von $\mathbf{A}_K$ schreiben wir I_K und nennen sie *Idelgruppe*. Die multiplikative Gruppe $K^\times$ ist eine Untergruppe von I_K. Die Quotientengruppe $C_K = I_K/K^\times$ nennen wir die *Idelklassengruppe*.

Wir machen I_K zu einer topologischen Gruppe, indem wir als Fundamentalsystem von Umgebungen von 1

$$\prod_{p \in S} W_\mathfrak{p} \times \prod_{\mathfrak{p} \notin S} U_\mathfrak{p}$$

nehmen mit S einer endlichen Menge, die alle Äquivalenzklassen von archimedischen Absolutbeträgen enthält, $U_\mathfrak{p} := \{x \in K_\mathfrak{p}^\times : |x|_\mathfrak{p} = 1\}$ und $W_\mathfrak{p}$ Umgebungen von 1 in $K_\mathfrak{p}^\times$. Die Idelklassengruppe C_K wird zur topologischen Gruppe mit der Quotiententopologie.

Ein Beispiel einer offenen Umgebung von 1 in I_K wäre die Untergruppe $I_K^{S_\infty} := \prod_{\mathfrak{p} \text{ arch.}} K_\mathfrak{p}^\times \times \prod_{\mathfrak{p} \text{ n.-arch.}} U_\mathfrak{p}$.

Lemma 5.16. *Jede offene Untergruppe einer topologischen Gruppe G ist auch abgeschlossen.*

Beweis. Sei $g \in G$. Die Abbildung $G \to G$, $x \mapsto gx$ ist ein Homöomorphismus. Wenn $H < G$ eine offene Untergruppe ist, muss gH eine offene Menge in G sein. Die Nebenklassen von H bilden eine Partition von G, und die Vereinigung aller Nebenklassen bis auf H ist offen. Also ist das Komplement von H offen. □

Somit ist $K^\times \cdot I_K^{S_\infty} = \bigcup_{k \in K^\times} k I_K^{S_\infty}$ offen. Die Untergruppe $C_K^1 := I_K^{S_\infty} \cdot K^\times / K^\times$ von C_K ist offen und nach dem Lemma abgeschlossen.

Sei K ein Zahlkörper und A dessen Ring der ganzen Zahlen. Seien $|\cdot|_\mathfrak{p}$ Repräsentanten der Äquivalenzklassen $\mathfrak{p}$ nicht-archimedischer Absolutbeträge von K. Das zu $|\cdot|_\mathfrak{p}$ *assoziierte Primideal* in der Gruppe J_K der Ideale in K sei $\mathfrak{p} := \{x \in A : |x|_\mathfrak{p} < 1\}$. Das Ideal $\mathfrak{p}$ ist prim, da es der Schnitt des maximalen Ideals in $\mathcal{O}_{|\cdot|_\mathfrak{p}}$ mit A ist. Wie bei einem Palimpsest, bei dem die abgekratzte Schrift noch immer etwas sichtbar ist, muss aus dem Kontext geschlossen werden, was wir mit $\mathfrak{p}$ meinen. Die Notation hat den Vorteil, dass das zu $|\cdot|_\mathfrak{p}$ assoziierte Primideal sofort gegeben ist.

Jedes Primideal $\mathfrak{q}$ von A ist das assoziierte Primideal eines Repräsentanten einer Äquivalenzklasse eines nicht-archimedischen Absolutbetrags von K. Sei nämlich $x \in A - \{0\}$ und $(x) = \prod_\mathfrak{q} \mathfrak{q}^{n_\mathfrak{q}}$ die Primfaktorisierung des von x erzeugten Hauptideals in A. Wir setzen $\nu_\mathfrak{q}(x) := n_\mathfrak{q}$ und $\nu_\mathfrak{q}\left(\frac{x}{y}\right) := \nu_\mathfrak{q}(x) - \nu_\mathfrak{q}(y)$ für $x \in A$ und $y \in A - \{0\}$; weiter setzen wir $\nu_\mathfrak{q}(0) := +\infty$. Die Funktion $|x| := N(\mathfrak{q})^{-\nu_\mathfrak{q}(x)}$ definiert einen Absolutbetrag auf K, dem Quotientenkörper von A, und es gilt $\mathfrak{q} = \{x \in A : |x| < 1\}$. Also induziert jedes Primideal in A einen Absolutbetrag. Wegen Lemma 5.14 sind $|\cdot|_\mathfrak{p}$ und $|x| = N(\mathfrak{p})^{-\nu_\mathfrak{p}(x)}$ äquivalent.

Sei $\mathfrak{q}$ ein Primideal in A. Die Funktion $\nu_\mathfrak{q}$ kann auf die Vervollständigung L von K bezüglich $|x| = N(\mathfrak{q})^{-\nu_\mathfrak{q}(x)}$ stetig erweitert werden; insbesondere ist noch immer $\nu_\mathfrak{q}(x) \in \mathbf{Z}$ für alle $x \in L$. Wir definieren nun einen Gruppenhomomorphismus $I_K \to J_K$ via

$$(x_\mathfrak{p}) \mapsto \prod_{\mathfrak{p} \text{ n.-arch.}} \mathfrak{p}^{\nu_\mathfrak{p}(x_\mathfrak{p})}.$$

Das Produkt ist endlich, da $x_\mathfrak{p} \in U_\mathfrak{p}$ ist für fast alle $\mathfrak{p}$, und die Abbildung ist surjektiv. Wir erhalten ferner einen Gruppenisomorphismus $I_K / I_K^{S_\infty} \cong J_K$. Ein Element $(x_\mathfrak{p}) \in I_K$ liegt in $\ker \phi'$ genau dann, wenn für alle nicht-archimedischen Äquivalenzklassen $\mathfrak{p}$ und alle $x_\mathfrak{p} \in K_\mathfrak{p}$ gilt, dass $\nu_\mathfrak{p}(x_\mathfrak{p}) = 0$ ist.

Satz 5.17. *Es gilt $I_K / (I_K^{S_\infty} \cdot K^\times) \cong H_K$.*

Beweis. Sei $(x_\mathfrak{p}) \in I_K$ so, dass $\phi'((x_\mathfrak{p})) = xA$ für ein $x \in K^\times$. Das heisst $\prod_{\mathfrak{p} \text{ n.-arch.}} \mathfrak{p}^{\nu_\mathfrak{p}(x_\mathfrak{p})} = xA$, was genau dann der Fall ist, wenn $\nu_\mathfrak{p}(x_\mathfrak{p}) = \nu_\mathfrak{p}(x)$ ist für alle nicht-archimedischen $\mathfrak{p}$. Wiederum heisst dies, dass $\nu_\mathfrak{p}(x_\mathfrak{p} x^{-1}) = 0$ ist. Schliesslich ist: $\phi'((x_\mathfrak{p})) = xA \Leftrightarrow (x_\mathfrak{p} x^{-1}) \in I_K^{S_\infty} \Leftrightarrow (x_\mathfrak{p}) \in x I_K^{S_\infty}$. Der Kern der Komposition $I_K \to J_K \to H_K$ ist folglich $I_K^{S_\infty} \cdot K^\times$, was zu beweisen war. □

So kommen wir zum Schluss dorthin, wo wir begonnen haben.

6. Klassenkörpertheorie

In diesem kurzen Abschnitt werden wir einzig die Sätze der Klassenkörpertheorie anführen, die wir benötigen, um den Beweis des Kummerschen Lemmas in Abschnitt 7 zu skizzieren. Die Sätze sind ziemlich kompliziert und ohne Kontext wären deren Beweise bloss eine lange Reihe algebraischer Manipulationen. (Ist ein Beweis, den eine Maschine formal überprüfen kann, auch ein Beweis für den menschlichen Leser?) Deswegen lassen wir die Beweise vollkommen weg.

Satz 6.1 (Existenzsatz)**.** *Es herrscht eine bijektive Korrespondenz zwischen den endlichen abelschen Erweiterungen L eines Zahlkörpers K und den abgeschlossenen Untergruppen von endlichem Index in der Idelklassengruppe C_K, gegeben durch $L \mapsto N_{L/K}(C_L)$, wobei $N_{L/K}(\alpha) = \prod_{\sigma\in\mathrm{Gal}(L/K)} \sigma(\alpha)$ für $\alpha \in C_L$.*

Der Beweis ist in [11, VII.12] zu finden.

Die Untergruppe C_K^1 von C_K ist abgeschlossen, wie wir oben gesehen haben. Nach Satz 5.17 ist C_K^1 von endlichem Index. Es gibt nach dem Existenzsatz also eine endliche abelsche Erweiterung K^1/K, so dass $N_{K^1/K}(C_{K^1}) = C_K^1$ ist.

Satz 6.2 (Artins globales Reziprozitätsgesetz)**.** *Für jede endliche Galois-Erweiterung L/K von Zahlkörpern gilt*

$$\mathrm{Gal}(L/K)^{ab} \cong C_K/N_{L/K}(C_L).$$

Die Darstellung der Sätze in diesem Abschnitt ist dem natürlichen Gedankengang der Klassenkörpertheorie nicht treu: für gewöhnlich wird das Artinsche Reziprozitätsgesetz im Beweis des Existenzsatzes gebraucht. Siehe [11, VII.3].

Im obigen Beispiel ist $\mathrm{Gal}(K^1/K) = \mathrm{Gal}(K^1/K)^{\mathrm{ab}} = C_K/C_K^1 \cong H_K$; der Grad der Körpererweiterung K^1/K ist mithin genau h_K. Die Erweiterung K^1 trägt den Namen *Hilbertscher Klassenkörper* von K.

Satz 6.3. *Sei L/K eine endliche unverzweigte abelsche Erweiterung eines Zahlkörpers K. Dann kann L in den Hilbertschen Klassenkörper von K eingebettet werden.*

Siehe [12, Ch. 8, Thm. 7]. Der Hilbertsche Klassenkörper von K ist selbst eine endliche unverzweigte abelsche Erweiterung von K.

7. Kummers Lemma

Das nachfolgende Lemma ist der schwierigste Teil von Kummers Beweis zu Fermats letztem Satz. Die letzten beiden Abschnitte gaben uns genügend Vokabular, um die Beweisidee zu geben. Es ist einiges mehr an algebraischer Zahlentheorie geboten, um den Beweis bis ins Detail auszuarbeiten. Wir folgen hier Serge Langs *Introduction to Cyclotomic Fields I and II* [19, Ch. 13, Thm. 6.1].

Wir werden den Begriff der *Differente* $\mathfrak{D}_{L/K}$ einer Erweiterung von Zahlkörpern L/K verwenden. Sei $\alpha \in L$ und $f \in K[X]$ das Minimalpolynom von α über K. Sei $\delta_{L/K}(\alpha) := f'(\alpha)$, falls $K(\alpha) = L$ ist, und sonst $\delta_{L/K}(\alpha) := 0$. Die Differente von L/K ist definiert als das Ideal $(\delta_{L/K}(\alpha) : \alpha \in B)$, wobei B der Ring der ganzen Zahlen von L ist. Ein Primideal $\mathfrak{P}$ im Ring der ganzen Zahlen von L ist genau dann verzweigt – soll heissen, dass $e(\mathfrak{P}) > 1$ ist –, wenn es die Differente teilt [5, II.2.6].

Eng verknüpft mit dem Begriff der Differente ist die *relative Diskriminante* von L/K. Sei A der Ring der ganzen Zahlen von K. Die relative Diskriminante ist definiert als das Ideal $\mathfrak{d}_{L/K}$ von A, welches durch die Diskriminanten aller in B gelegener Basen des K-Vektorraumes L erzeugt werden. Die relative Diskriminante $\mathfrak{d}_{L/K}$ steht deswegen in enger Beziehung zur Differente $\mathfrak{D}_{L/K}$, weil $\mathfrak{d}_{L/K} = N_{L/K}(\mathfrak{D}_{L/K})$ gilt [5, Kap. III, Thm. 2.9]. Ein Primideal $\mathfrak{p}$ in A ist genau dann verzweigt in B, wenn es die relative Diskriminante $\mathfrak{d}_{L/K}$ teilt [5, Kap. III, Kor. 2.12].

Lemma 7.1 (Kummers Lemma)**.** *Sei p eine reguläre Primzahl und ξ eine primitive p-te Einheitswurzel. Wenn u eine Einheit in $\mathbf{Z}[\xi]$ ist und $u \equiv a \pmod{p}$ ist für eine ganze Zahl a, dann enthält $\mathbf{Z}[\xi]$ eine p-te Wurzel von u.*

Beweisidee. Sei $K := \mathbf{Q}(\xi)$. Wir brauchen nur zu zeigen, dass eine p-te Wurzel von u in K liegt. Sei nämlich $g(X)$ ein normiertes Polynom mit ganzzahligen Koeffizienten, so dass $g(u) = 0$ ist. Dann ist jede p-te Wurzel von u Nullstelle von $g(X^p)$ und somit im Ring der ganzen Zahlen von K enthalten.

Wir betrachten die Erweiterung $K(u^{1/p})$. Das Lemma ist bewiesen, wenn $K(u^{1/p})$ als unverzweigt über K nachgewiesen werden kann. Dann kann $K(u^{1/p})$ nämlich in den Hilbertschen Klassenkörper K^1 von K eingebettet werden und $[K(u^{1/p}) : K]$ teilt $[K^1 : K] = h_p$. Nun ist aber $K(u^{1/p})$ ein Zerfällungskörper von $X^p - u$ über K. Je nachdem, ob K eine p-te Wurzel von u enthält oder nicht, zerfällt das Polynom in Linearfaktoren oder ist irreduzibel. Der Grad der Erweiterung $[K(u^{1/p}) : K]$ ist also 1 oder p. Es kann aber nicht p sein, da p als regulär vorausgesetzt wurde, also h_p nicht teilt. Also ist $u^{1/p} \in K$.

Falls $[K(u^{1/p}) : K] = 1$ ist, sind alle Primideale unverzweigt. Wir nehmen also an, dass $[K(u^{1/p}) : K] = p$ ist. Eine Basis von $K(u^{1/p})$ als K-Vektorraum ist gegeben durch $1, u^{1/p}, \xi u^{1/p}, \xi^2 u^{1/p}, ..., \xi^{p-2} u^{1/p}$. Diese Basis liegt im Ring der ganzen Zahlen von $K(u^{1/p})$, da $u^{1/p}$ ganz über $\mathbf{Z}[\xi]$ ist und somit ganz über $\mathbf{Z}$ nach [1, Cor. 5.4]. Die Diskriminante $D(1, u^{1/p}, \xi u^{1/p}, \xi^2 u^{1/p}, ..., \xi^{p-2} u^{1/p})$ ist gleich

$$\det\left((u^{1/p}\xi^{(j-1)i})_{i,j}\right)^2 = \det(\mathrm{diag}(u^{1/p}, ..., u^{1/p})^2 \cdot \det(1, \xi, \xi^2, ..., \xi^{p-2})^2 = \pm\left(u^{1/p}\right)^{2p} p^{p-2} = \pm u^2 p^{p-2}$$

nach Gleichung (3.1). Die relative Diskriminante von $K(u^{1/p})/K$ ist also in $(p)^{p-2} \subset (1-\xi)$ enthalten. Somit ist $(1-\xi)$ das einzige Primideal in K, das in $K(u^{1/p})$ verzweigt sein könnte.

Nach Fermats kleinem Satz ist $u^{p-1} \equiv a^{p-1} \equiv 1 \pmod{p}$. Sei v eine p-te Wurzel von u^{p-1}. Dann ist $v^{-1}u$ eine p-te Wurzel von u. Also kann, indem wir u durch u^{p-1} ersetzen, o.B.d.A. angenommen werden, dass $u \equiv 1 \pmod{p}$ ist.

Wir verwenden die Voraussetzung $u \equiv 1 \pmod{p}$, um die Unverzweigheit von $(1-\xi)$ in $K(u^{1/p})$ zu zeigen:

Nach Korollar 3.4 ist ein beliebiges Element von $\mathbf{Z}[\xi]$ modulo $(1-\xi)$ kongruent zu einer ganzen Zahl. Es gilt $u-1 = py$ für ein $y \in \mathbf{Z}[\xi]$ nach Voraussetzung. Seien $m \in \mathbf{Z}$ und $x \in \mathbf{Z}[\xi]$ so, dass $y = m+(1-\xi)x$ ist. Somit ist $u = 1 + pm + p(1-\xi)x = 1 + pm + (1-\xi)^p x$. Dies gibt:

$$\begin{aligned} 1 = N_{\mathbf{Q}(\xi)/\mathbf{Q}}(u) &= \prod_{\sigma \in \mathrm{Gal}(\mathbf{Q}(\xi)/\mathbf{Q})} \left(1 + pm + \sigma\left(p(1-\xi)x\right)\right) \\ &\equiv (1+pm)^{p-1} \equiv 1 + (p-1)pm \equiv 1 - pm \pmod{(1-\xi)^p}, \end{aligned}$$

da $\sigma(1-\xi)$ von der Form $1-\xi^r$ mit $1 \le r < p$ ist und $(1-\xi)$ das Ideal $(\sigma(1-\xi))$ teilt. Folglich ist $u = 1 + pm + (1-\xi)^p x \equiv 1 \pmod{(1-\xi)^p}$.

Das Polynom

$$f(X) = \frac{1}{(1-\xi)^p}\left((1-\xi)X+1)^p - u\right)$$

ist normiert und hat Koeffzienten in $\mathbf{Z}[\xi]$, da $u-1$ durch $(1-\xi)^p$ teilbar ist und $\binom{p}{k}$ durch p und also durch $(1-\xi)^{p-1}$ teilbar ist für $0<k<p$. Die Nullstellen von f sind $\frac{u^{1/p}-1}{1-\xi}$, $\frac{\xi u^{1/p}-1}{1-\xi}$, $\frac{\xi^2 u^{1/p}-1}{1-\xi}$, ..., $\frac{\xi^{n-1}u^{1/p}-1}{1-\xi}$. Sei β eine beliebige Nullstelle von f. Es ist $K(\beta)=K(u^{1/p})$ und es gilt die Gleichung

$$f'(\beta) = \frac{p}{(1-\xi)^{p-1}}\left((1-\xi)\beta+1\right)^{p-1} \equiv 1 \pmod{(1-\xi)}.$$

Also sind die Ideale $(f'(\beta))$ und $(1-\xi)$ koprim. Jedoch ist $(f'(\beta))$ in der Differente von $K(u^{1/p})/K$ enthalten. Mithin ist kein Primideal, das $(1-\xi)$ teilt, verzweigt. □

8. Eulers Beweis für n = 3

An dieser Stelle kehren wir zu elementaren Betrachtungen zurück, die auf Euler zurückgehen. Das Vokabular, das wir uns erarbeitet haben, werden wir jedoch weiterhin verwenden.

Der Beweis von Fermats letztem Satz für reguläre Primzahlen im nächsten Abschnitt wird den Fall $n=3$ ausschliessen müssen. Zuerst zeigen wir, dass 3 eine reguläre Primzahl ist:

Satz 8.1. *Sei ω eine primitive dritte Einheitswurzel. Die Klassenzahl von $\mathbf{Q}(\omega)$ ist gleich* 1.

Beweis. Eine Ganzheitsbasis von $\mathbf{Q}(\omega)$ ist gegeben durch 1 und ω. Seien $\alpha,\beta\in\mathbf{Z}[\omega]$ gegeben; dann existiert ein $\gamma\in\mathbf{Z}[\omega]$, so dass $\left|N_{\mathbf{Q}(\omega)/\mathbf{Q}}\left(\frac{\alpha}{\beta}-\gamma\right)\right|<1$ ist.

In der Tat: Für $x,y\in\mathbf{Q}$ ist $N_{\mathbf{Q}(\omega)/\mathbf{Q}}(x+y\omega)=x^2-xy+y^2$, und wählen wir $a,b\in\mathbf{Z}$ so, dass $|x-a|,|y-b|<\frac{1}{2}$ sind, dann ist

$$\left|N_{\mathbf{Q}(\omega)/\mathbf{Q}}\left(x+y\omega-(a+b\omega)\right)\right| \le (x-a)^2+(x-a)(y-b)+(y-b)^2 < 1.$$

Wählen wir nun $x,y\in\mathbf{Q}$ so, dass $x+y\omega=\frac{\alpha}{\beta}$ ist, ist das gesuchte γ durch $a+b\omega$ gegeben.

Also ist $\left|N_{\mathbf{Q}(\omega)/\mathbf{Q}}(\alpha-\beta\gamma)\right| < \left|N_{\mathbf{Q}(\omega)/\mathbf{Q}}(\beta)\right|$ und damit $\mathbf{Z}[\omega]$ ein euklidischer Ring mit Bewertungsfunktion $\left|N_{\mathbf{Q}(\omega)/\mathbf{Q}}(\cdot)\right|$. Mit Korollar 4.5 folgt die Behauptung. □

Man bemerke, dass $\mathbf{Q}(\sqrt{-3})=\mathbf{Q}(\omega)$ ist, da $\frac{1}{2}(1+\sqrt{-3})$ eine primitive dritte Einheitswurzel ist. Der Ring der ganzen Zahlen von $\mathbf{Q}(\sqrt{-3})$ ist folglich $\mathbf{Z}[\frac{1}{2}(1+\sqrt{-3})]$ und nicht $\mathbf{Z}[\sqrt{-3}]$. Letzterer ist nicht einmal ein faktorieller Ring.

Lemma 8.2. *Die Einheitengruppe von $\mathbf{Z}[\omega]$ ist $\{\pm1,\pm\omega,\pm\omega^2\}$.*

Beweis. Jede Einheit $a+b\omega$ mit $a,b\in\mathbf{Z}$ erfüllt $N_{\mathbf{Q}(\omega)/\mathbf{Q}}(a+b\omega)=a^2-ab+b^2=\pm1$; somit ist auch $|a+b\omega|^2=(a+b\omega)(a-b\omega)=a^2-ab+b^2=1$ mit $|\cdot|$ dem üblichen Absolutbetrag auf $\mathbf{C}$. Also muss jede Einheit in $a+b\omega$ eine Einheitswurzel sein. Diese sind in $\mathbf{Q}(\omega)$, wie wir in Abschnitt 3 gezeigt haben, genau $\{\pm1,\pm\omega,\pm\omega^2\}$. □

Der Beweis von Fermats letztem Satz im Fall $n=3$, den wir geben werden, ist ursprünglich in Eulers *Vollständige Anleitung zur Algebra* II.243 [13] zu finden. Euler sah die Aussage von Lemma 8.4 dieses Textes als offensichtlich an, – was sie auch wäre, wenn der Ring $\mathbf{Z}[\sqrt{-3}]$ faktoriell wäre. Wir beweisen das Lemma rigoros, wobei wir [14] folgen werden.

Unter einem *Kubus* in einem Ring A verstehen wir ein Element $x \in A$, so dass ein Element $y \in A$ existiert mit $x = y^3$. Wir verwenden in Anlehnung an Euler den altmodischen Ausdruck „Kubus“ um des Charmes der Mathematik vergilbter Bücher willen.

Zuerst ein simples Lemma:

Lemma 8.3. *Sei x ein Kubus in $\mathbf{Z}$. Seien q eine Primzahl und $0 < a < q^3$ so, dass $x \equiv a \pmod{q^3}$ ist. Dann teilt q die Zahl a nicht.*

Beweis. Angenommen q teilt die Zahl a. Dann ist $x \equiv 0 \pmod{q}$. Da x also von der Primzahl q geteilt wird und x ein Kubus ist, muss $q^3 \mid x$ gelten. Dies widerspricht der Annahme, dass $0 < a < q^3$ ist. □

Lemma 8.4. *Seien x und y teilerfremde ganze Zahlen, so dass $x^2 + 3y^2$ ein Kubus in $\mathbf{Z}$ ist. Dann ist $x + \sqrt{-3}y$ ein Kubus in $\mathbf{Z}[\sqrt{-3}]$.*

Beweis. Zuerst sei angemerkt, dass nicht beide x und y gerade sein können, da sie teilerfremd sind. Sie können auch nicht beide ungerade sein. Wäre dem nämlich so, dann wäre $x^2 + 3y^2 \equiv 4 \pmod{8}$ und wegen des vorherigen Lemmas kann $x^2 + 3y^2$ kein Kubus sein.

Zusätzlich muss gelten, dass $\mathrm{ggT}(3, x) = 1$ ist. Nehmen wir widerspruchsweise an, dass x durch 3 teilbar ist. Falls $y^2 \equiv 0, 3, 6 \pmod{9}$ ist, so ist y durch 3 teilbar, was wegen der Teilerfremdheit von x und y nicht sein kann. Falls $y^2 \equiv 2, 5, 8 \pmod{9}$ ist, dann ist $x^2 + 3y^2 \equiv 6 \pmod{9}$ und $x^2 + 3y^2$ kann wegen dem vorherigen Lemma kein Kubus sein. Schliesslich, falls $y^2 \equiv 1, 4, 7 \pmod{9}$ ist, dann ist $x^2 + 3y^2 \equiv 3 \pmod{9}$ und wiederum wegen dem vorherigen Lemma kann $x^2 + 3y^2$ kein Kubus sein.

Wir schreiben $x^2 + 3y^2 = (x + \sqrt{-3}y)(x - \sqrt{-3}y)$ in $\mathbf{Z}[\omega]$. Die Elemente $x + \sqrt{-3}y$ und $x - \sqrt{-3}y$ sind koprim in $\mathbf{Z}[\omega]$, da ein Ideal, welches beide Elemente enthielte, auch $2x$ und $x^2 + 3y^2$ enthielte; letzteres ist eine ungerade ganze Zahl, da genau eine der Zahlen x und y ungerade ist, und das Ideal müsste x und $x^2 + 3y^2$ enthalten. Das heisst aber auch, dass besagtes Ideal x^2 und $3y^2$ enthielte, was nur das Einsideal sein kann, da x mit 3 und y teilerfremd ist.

Wir schreiben also $x + \sqrt{-3}y = u(a + b\omega)^3$ für eine Einheit $u \in \mathbf{Z}[\omega]$ und $a, b \in \mathbf{Z}$. Wir verwenden hier, dass $\mathbf{Z}[\omega]$ faktoriell ist – das Argument wäre in $\mathbf{Z}[\sqrt{-3}]$ ungültig. Jeder Kubus z in einem faktoriellen Ring ist nämlich als $p_1^3 \cdots p_r^3$ schreibbar für irreduzible Elemente $p_1, ..., p_r$ mit $r \geq 1$. Wenn also $z = z_1 z_2$ ein Kubus ist und z_1 und z_2 teilerfremd sind, so kommt jedes p_i^3 entweder in der Primfaktorisierung von z_1 oder in z_2 vor. Somit sind z_1 und z_2 wiederum Kuben.

Das Element $a + b\omega$ lässt sich als $\frac{a_1}{2} + \frac{b}{2}\sqrt{-3}$ mit $a_1 = 2a + b$ schreiben, wenn wir $\omega := \frac{1}{2}(1 + \sqrt{-3})$ als Einheitswurzel nehmen. Man bemerke, dass $a_1 \equiv b \pmod{2}$ ist, also sind a_1, b entweder beide gerade oder beide ungerade.

Falls beide ungerade sind, können wir $c, d \in \{\pm 1\}$ wählen mit $a_1 \equiv c \pmod{4}$ und $b \equiv d \pmod{4}$. Wir erhalten

$$\left(\frac{a_1}{2} + \frac{b}{2}\sqrt{-3}\right) \cdot \left(\frac{c}{2} - \frac{d}{2}\sqrt{-3}\right) = \frac{1}{4}(a_1 c + 3bd) + \frac{1}{4}(bc - a_1 d)\sqrt{-3}.$$

Weil $a_1 c + 3bd \equiv c^2 + 3d^2 \equiv 0 \pmod{4}$ und $bc - a_1 d \equiv 0 \pmod{4}$ gilt, erhalten wir

$$\left(\frac{a_1}{2} + \frac{b}{2}\sqrt{-3}\right) \cdot \left(\frac{c}{2} - \frac{d}{2}\sqrt{-3}\right) \in \mathbf{Z}[\sqrt{-3}] \subset \mathbf{Z}[\omega].$$

Allerdings ist $v := \left(\frac{c}{2} - \frac{d}{2}\sqrt{-3}\right) \in \mathbf{Z}[\omega]$ eine Einheit, da es eines der folgenden Elemente sein muss: $\omega = \frac{1}{2} + \frac{1}{2}\sqrt{-3}$, $\omega^2 = \overline{\omega} = \frac{1}{2} - \frac{1}{2}\sqrt{-3}$, $-\omega = -\frac{1}{2} - \frac{1}{2}\sqrt{-3}$ oder $-\overline{\omega} = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$.

Deswegen können wir $x + \sqrt{-3}y = (k + \sqrt{-3}l)^3\varepsilon$ für gewisse $k, l \in \mathbf{Z}$, schreiben, wobei $\varepsilon = uv^{-3}$ ist. Falls $a_1 \equiv b \equiv 0 \pmod 2$ ist, hat $x + \sqrt{-3}y$ dieselbe Form, ausser dass dort $\varepsilon = u$ ist.

Wir zeigen nun, dass ε eine reelle Einheit sein muss. Sei $\varepsilon^{-1} = e + f\omega$ für $e, f \in \mathbf{Z}$; also ist

$$\varepsilon^{-1}(x + \sqrt{-3}y) = xe + \frac{1}{2}(xf - 3yf) + \sqrt{-3}\left(ye + \frac{1}{2}(xf + yf)\right) \in \mathbf{Z}[\sqrt{-3}].$$

Genau eine der Zahlen x, y ist gerade und $\frac{1}{2}(xf + yf)$ ist eine ganze Zahl. Somit ist f eine gerade Zahl. Nach Lemma 8.2 muss dann aber $\varepsilon^{-1} = \pm 1$ sein. □

Wir bringen das Lemma noch auf die Form, die uns im Beweis hilfreich sein wird:

Lemma 8.5. *Seien $x, y \neq 0$ teilerfremde ganze Zahlen, so dass $x^2 + 3y^2$ ein Kubus ist und x nicht durch 3 teilbar und y ungerade ist.*
Falls $2x$ ein Kubus in $\mathbf{Z}$ ist, so existiert ein gerader Kubus, der $2x$ teilt und die Summe zweier von null verschiedener Kuben ist.
Falls $\frac{2y}{3}$ ein Kubus in $\mathbf{Z}$ ist, so existiert ein gerader Kubus, der $2y$ teilt und der die Summe zweier von Null verschiedener Kuben ist.

Beweis. Nach dem vorherigen Lemma ist $x + \sqrt{-3}y = (s + \sqrt{-3}r)^3$ für gewisse $r, s \in \mathbf{Z}$. Also ist

$$x + \sqrt{-3}y = r^3 - 9rs^2 + \sqrt{-3}\left(3r^2s - 3s^3\right)$$

und somit $x = r^3 - 9rs^2 = r(r + 3s)(r - 3s)$ und $y = 3r^2s - 3s^3 = 3s(r - s)(r + s)$.

Da x nicht durch 3 teilbar ist, ist r auch nicht durch 3 teilbar; und weil y ungerade ist, so sind auch s und $r^2 - s^2$ ungerade. Dies heisst wiederum, dass r gerade ist.

Die ganzen Zahlen $2r$, $r + 3s$ und $r - 3s$ sind paarweise teilerfremd, wie sich leicht nachprüfen lässt. Zum Beispiel: Wenn $r - 3s$ und $r + 3s$ einen gemeinsamen Faktor hätten, teilte derselbe Faktor auch $2r$ und $6s$. Dieser kann aber nicht 2 sein, da $r + 3s, r - 3s$ beide ungerade sind. Da r auch nicht durch 3 teilbar ist, müssten r, s einen gemeinsamen Faktor haben. Dies widerspräche aber der Teilerfremdheit von x und y.

Auch gilt wegen ähnlicher Argumente, dass für $s(r - s)(r + s)$ die Faktoren s und $r - s$ und $r + s$ paarweise teilerfremd sind.

Wenn nun $2x$ ein Kubus ist, so ist wegen $2x = 2r(r + 3s)(r - 3s)$ auch $2r$ ein Kubus, der Summe der Kuben $r + 3s$ und $r - 3s$ ist.

Wenn $\frac{2}{3}y$ ein Kubus ist, so ist wegen $\frac{2}{3}y = 2s(r + s)(r - s)$ auch $2s$ ein Kubus, der Summe der Kuben $r + s$ und $r - s$ ist. □

Satz 8.6. *Es kann keine zwei Kuben in $\mathbf{Z}$ geben, die nicht Null sind und deren Summe ein Kubus ist, der nicht Null ist.*

Beweis. Angenommen es gäbe ganze Zahlen x, y, z, alle nicht Null, welche $x^3 + y^3 = z^3$ erfüllen. Falls z ungerade ist, dann ist genau eine der Zahlen x, y ungerade. Sagen wir, y sei gerade. Dann ist also $x^3 + (-z)^3 = (-y)^3$ und durch Multiplikation der Gleichung mit -1 (falls notwendig) erhalten wir eine

positive ganze Zahl auf der rechten Seite der Gleichung. Wir können also o.B.d.A. annehmen, dass z gerade und positiv ist.

Sei $z \geq 1$ die kleinste gerade Zahl, welche die Gleichung erfüllt. Die Zahlen x, y sind teilerfremd, denn andernfalls könnten wir die Gleichung durch $\mathrm{ggT}(x, y)$ teilen und erhielten einen Widerspruch zur Minimalität von z. Da z gerade ist, müssen x und y ungerade sein.

Seien $p = \frac{1}{2}(x+y)$, $q = \frac{1}{2}(x-y)$. Da $x = p+q$ und $y = p-q$ sind, sind die Zahlen p und q teilerfremd und genau eine der beiden ist ungerade. Die Gleichung $z^3 = y^3 + x^3$ transformiert sich in

$$z^3 = x^3 + y^3 = 2p^3 + 6pq^2 = 2p(p^2 + 3q^2)$$

Die Zahl $p^2 + 3q^2$ ist ungerade; da z^3 durch 8 teilbar ist, ist p durch 4 teilbar.

Angenommen 3 teilt p nicht: Dann sind $2p$ und p^2+3q^2 teilerfremd, denn wären beide im selben Ideal von $\mathbf{Z}$ enthalten, so enthielte dieses $4p^2$ und p^2+3q^2 und also auch p^2 und $3q^2$, da p^2+3q^2 ungerade ist. Da p nicht durch 3 teilbar ist, enthielte das Ideal also p^2 und q^2, was nur das Einsideal sein kann. Also sind $2p$ und $p^2 + 3q^2$ beides Kuben.

Angenommen nun, dass p durch 3 teilbar ist. Schreiben wir $p = 3t$ erhalten wir:

$$z^3 = 6t(9t^2 + 3q^2) = 18t(3t^2 + q^2)$$

Dividieren wie die Gleichung durch 27, sehen wir, dass $\frac{2}{3}t(q^2 + 3t^2)$ ein Kubus ist. Die Zahlen t, q sind teilerfremd, weil p und q teilerfremd waren. Weil $q^2 + 3t^2 \equiv (x-y)^2 \equiv 1, 2 \pmod 3$ gilt, ist t durch 3 teilbar. Die ganzen Zahlen $\frac{2t}{3}$ und $q^2 + 3t^2$ sind teilerfremd und somit Kuben.

Beide Fälle geben nach Lemma 8.5 eine im Betrag kleinere Zahl als z, welche ebenfalls gerade und Summe zweier Kuben ist. Dieser Widerspruch beschliesst den Beweis. □

9. Kummers Beweis des Fermatschen Satzes für reguläre Primzahlen

Satz 9.1 (Kummer)**.** *Sei $p \geq 5$ eine reguläre Primzahl und ξ eine primitive p-te Einheitswurzel. Sei u eine Einheit in $\mathbf{Z}[\xi]$ und $n \geq 0$ eine ganze Zahl. Es existieren keine teilerfremden postiven ganzen Zahlen $x, y, z \not\equiv 0 \pmod p$, so dass*

$$x^p + y^p = u(1-\xi)^{np} z^p$$

gilt.

Sei zuerst $n = 0$. Da $u = \frac{x^p+y^p}{z^p}$ in $\mathbf{Q} \cap \mathbf{Z}[\xi] = \mathbf{Z}$ liegt und eine Einheit in $\mathbf{Z}[\xi]$ ist, muss $u = \pm 1$ sein. Wir können o.B.d.A. annehmen, dass $u = 1$ ist, ansonsten betrachten wir die Gleichung $x^p + y^p = (-z)^p$.

Wegen $x^p + y^p = (x+y)(x+\xi y)(x+\xi^2 y)\cdots(x+\xi^{p-1}y)$ erhalten wir die Gleichung

$$z^p = (x+y)(x+\xi y)(x+\xi^2 y)\cdots(x+\xi^{p-1}y). \tag{9.1}$$

Lemma 9.2. *Sei $p \geq 3$ eine Primzahl und ξ eine primitive p-te Einheitswurzel. Seien $x, y \in \mathbf{Z}$ nicht Null und teilerfremd. Seien $0 \leq i < j \leq p-1$. Dann ist $(1-\xi)$ das einzige maximale Ideal, das beide Ideale $(x+\xi^i y)$ und $(x+\xi^j y)$ in $\mathbf{Z}[\xi]$ teilen kann.*

Beweis. Sei $\mathfrak{p}$ ein maximales Ideal in $\mathbf{Z}[\xi]$, welches $(x+\xi^i y)$ und $(x+\xi^j y)$ enthält. Dann enthält $\mathfrak{p}$ auch $\xi^i \frac{1-\xi}{1-\xi^{j-i}}(x+\xi^i y - (x+\xi^j y)) = (1-\xi)y$ und $\xi^j \frac{1-\xi}{1-\xi^{i-j}}\left(\xi^j(x+\xi^i y) - \xi^i(x+\xi^j y)\right) = \frac{1-\xi}{\xi^j-\xi^i}(\xi^j - \xi^i)x = (1-\xi)x$. Also ist entweder $1-\xi \in \mathfrak{p}$ oder $x, y \in \mathfrak{p}$. Letzteres kann nicht sein, da x, y teilerfremd sind. □

Lemma 9.3. *Sei $p \geq 5$ eine reguläre Primzahl und $x, y, z \not\equiv 0 \pmod{p}$ teilerfremde positive ganze Zahlen, so dass $x^p + y^p = z^p$ ist. Dann ist $x \equiv y \pmod{p}$.*

Beweis. Falls der $\mathrm{ggT}(x, y) > 1$ ist, muss wegen $x^p + y^p = z^p$ auch z durch den $\mathrm{ggT}(x, y)$ teilbar sein, was der Teilerfremdheit von x, y und z widerspricht. Also sind x und y teilerfremd.

Die Ideale $(x+y), (x+\xi y), ..., (x+\xi^{p-1}y)$ sind nach Lemma 9.2 paarweise koprim, da z nicht in $(1-\xi)$ liegt, - schliesslich liegt eine ganze Zahl genau dann in $(1-\xi)$, wenn sie durch p teilbar ist. Jedes Ideal $(x+y), (x+\xi y), ..., (x+\xi^{p-1}y)$ muss dann wegen der eindeutigen Primfaktorisierung von Idealen eine p-te Potenz sein. Da p regulär ist, ist der p-Torsionsanteil der Klassengruppe trivial; also ist $(x+\xi^i y)$ die p-te Potenz eines Hauptideals. Sei $\alpha_i \in \mathbf{Z}[\xi]$ so, dass $(\alpha_i)^p = (x+\xi^i y)$ ist für alle $0 \leq i \leq p-1$. Insbesondere existiert ein $v_i \in \mathbf{Z}[\xi]^\times$, so dass $v_i \alpha_i^p = x + \xi^i y$ ist.

Wegen Satz 3.9 können wir auch $v_1 = \xi^r v_1'$ schreiben für ein $r \in \mathbf{Z}$ und ein $v_1' \in \mathbf{R}$. Die p-te Potenz eines Elements von $\mathbf{Z}[\xi]$ ist eine ganze Zahl modulo p, also ist $x + \xi y = v_1' \xi^r \alpha_1^p \equiv v_1' \xi^r a \pmod{p}$ für ein $a \in \mathbf{Z}$. Betrachten wir das komplex Konjugierte von $x + \xi y$, ergibt dies $x + \xi^{-1} y \equiv v_1' \xi^{-r} \overline{\alpha_1}^p \equiv v_1' \xi^{-r} a \pmod{p}$. Somit ist

$$\xi^r (x + \xi^{-1} y) \equiv \xi^{-r} (x + \xi y) \pmod{p}. \tag{9.2}$$

Falls r von p geteilt würde, wäre $x + \xi^{-1} y \equiv x + \xi y \pmod{p}$ und weiter $(\xi - \xi^{-1}) y \equiv 0 \pmod{p}$, was $(1-\xi) y \in (1-\xi)^{p-1}$ und $y \in (1-\xi)^{p-2} \subset (1-\xi)$ bedeuten würde. Dies kann also nicht sein.

Falls $r \equiv 1 \pmod{p}$ wäre, so folgte aus Gleichung (9.2) $(\xi - \xi^{-1}) x \equiv 0 \pmod{p}$. Da $\frac{1-\xi^2}{1-\xi}$ eine Einheit ist in $\mathbf{Z}[\xi]$ nach Lemma 3.1, folgt $x \in (1-\xi)^{p-2} \subset (1-\xi)$ im Widerspruch zur Voraussetzung.

Also ist keines der $\xi^r, \xi^{r-1}, \xi^{1-r}$ und ξ^{-r} gleich 1. Da $\xi, \xi^2, ..., \xi^{p-1}$ eine $\mathbf{Q}$-Basis von $\mathbf{Q}(\xi)$ bildet und da $p \geq 5$ ist, sind $\xi^r, \xi^{r-1}, \xi^{1-r}$ und ξ^{-r} linear unabhängig, wenn sie paarweise verschieden sind. Dies ist nur der Fall, wenn $2r \not\equiv 1 \pmod{p}$ ist.

Nehmen wir an, dass $2r \not\equiv 1 \pmod{p}$ ist, also dass $\xi^r, \xi^{r-1}, \xi^{1-r}$ und ξ^{-r} linear unabhängig über $\mathbf{Q}$ sind. Wir hätten

$$\xi^r (x + \xi^{-1} y) - \xi^{-r} (x + \xi y) = \xi^r x + \xi^{r-1} y - \xi^{-r} x + \xi^{1-r} y \equiv 0 \pmod{p}.$$

Dann wäre $\xi^r \frac{x}{p} + \xi^{r-1} \frac{y}{p} - \xi^{-r} \frac{x}{p} + \xi^{1-r} \frac{y}{p} \in \mathbf{Z}[\xi]$, was wiederum $\frac{x}{p} \in \mathbf{Z}$ hiesse im Widerspruch zu $x \notin (1-\xi)$.

Also muss $2r \equiv 1 \pmod{p}$ sein. Wegen Gleichung (9.2) erhalten wir

$$(\xi - 1)(x - y) \equiv 0 \pmod{p}.$$

Also ist $x - y$ im Ideal $(1-\xi)$ enthalten und weil $x - y$ eine ganze Zahl ist, ist $x - y \equiv 0 \pmod{p}$. □

Wenn wir Lemma 9.3 auf die Gleichung $x^p + y^p = z^p$ und auf die äquivalente Gleichung $x^p + (-z)^p = (-y)^p$ anwenden, erhalten wir $x \equiv y \pmod{p}$ und $x \equiv -z \pmod{p}$. Also ist

$$2x^p \equiv x^p + y^p = z^p \equiv -x^p \pmod{p}.$$

Somit ist $3x^p \equiv 0 \pmod{p}$, was zu einem Widerspruch führt, da $p > 3$ ist und x nicht von p geteilt wird. Dies beweist Satz 9.1 im Falle $n = 0$.

Sei nun $n > 0$. Wir nehmen nun als schwächere Voraussetzung in Satz 9.1 an, dass x, y und z in $\mathbf{Z}[\xi]$ (aber nicht unbedingt in $\mathbf{Z}$) liegen und dass $x, y, z \notin (1-\xi)$ sind. Gesetzt, es existieren $x, y, z \notin (1-\xi)$, so dass $x^p + y^p = u(1-\xi)^{np} z^p$ ist.

Für alle $r > 0$ gilt, dass

$$x + \xi^r y \equiv x + y - ry(1-\xi) \pmod{(1-\xi)^2} \tag{9.3}$$

ist, wie sich leicht durch Induktion nach r zeigen lässt. Seien $a, b \in \mathbf{Z}$ so, dass $x \equiv a + b(1-\xi) \pmod{(1-\xi)^2}$ ist. Da x nicht in $(1-\xi)$ liegt, liegt auch a nicht in $(1-\xi)$, was wiederum bedeutet, dass a nicht durch p teilbar ist. Sei $h \in \mathbf{Z}$. Aus Gleichung (9.3) folgt $\xi^h \equiv 1 - h(1-\xi) \pmod{(1-\xi)^2}$. Damit erhalten wir $\xi^h x \equiv a + (b - ah)(1-\xi) \pmod{(1-\xi)^2}$. Sei $c \in \mathbf{Z}$ so, dass $ac \equiv 1 \pmod{p}$. Dann gilt $\xi^{bc} x \equiv a \pmod{(1-\xi)^2}$.

Wenn wir nun x durch $\xi^{bc} x$ ersetzen, so ist die Gleichung $x^p + y^p = u(1-\xi)^{np} z^p$ noch immer erfüllt, da $\left(\xi^{bc}\right)^p = 1$ ist. Wir können also o.B.d.A. annehmen, dass x (und mit derselben Argumentation auch y) zu einer ganzen Zahl kongruent ist modulo $(1-\xi)^2$. Seien $x_0, y_0 \in \mathbf{Z}$ so, dass $x \equiv x_0 \pmod{(1-\xi)^2}$ und $y \equiv y_0 \pmod{(1-\xi)^2}$ ist. Insbesondere sind $x_0, y_0 \neq 0$.

Weil wir $n > 0$ angenommen haben und weil die Gleichung von Idealen

$$(x+y)(x+\xi y)(x+\xi^2 y) \cdots (x+\xi^{n-1} y) = (1-\xi)^{np} (z^p)$$

gilt, muss es ein r geben, so dass $(x + \xi^r y)$ durch $(1-\xi)$ teilbar ist. Dann ist

$$x_0 + y_0 \equiv x_0 + y_0 - r y_0 (1-\xi) \equiv x + \xi^r y \equiv 0 \pmod{(1-\xi)}.$$

Da nach (9.3) die Gleichung $x + \xi^i y \equiv x_0 + y_0 \pmod{(1-\xi)}$ aber für alle $0 \leq i < p$ gilt, ist das Ideal $(x + \xi^i y)$ für alle $0 \leq i < p$ durch $(1-\xi)$ teilbar.

Da $x_0 + y_0$ eine ganze Zahl ist, muss $x_0 + y_0 \equiv 0 \pmod{p}$ sein, und schwächer: $x_0 + y_0 \equiv 0 \pmod{(1-\xi)^2}$. Es gilt also – wiederum nach (9.3) – die Gleichung $x + \xi^i y \equiv i y_0 (1-\xi) \pmod{(1-\xi)^2}$ für alle $1 \leq i < p$. Das heisst aber, dass $x + y \equiv 0 \pmod{(1-\xi)^2}$ ist. Hernach ist das Ideal $(x+y)$ durch $(1-\xi)^2$ teilbar.

Dies zeigt uns schon, dass $n = 1$ nicht sein kann, denn dann wäre $u(1-\xi)^p z^p = x^p + y^p \in (1-\xi)^{p+1}$, was wegen $z \notin (1-\xi)$ nicht sein kann.

Nehmen wir also an, dass $n > 1$ ist, und nehmen wir als Induktionshypothese an, dass der Satz 9.1 für $n-1$ unter der abgeschwächten Voraussetzung $x, y, z \in \mathbf{Z}[\xi]$ gilt.

Weil $x + \xi^r y \equiv iy(1-\xi) \pmod{(1-\xi)^2}$ für alle $1 \leq i \leq p-1$ gilt, aber i, y nicht in $(1-\xi)$ enthalten sind, ist $x + \xi^i y$ mit $1 \leq i \leq p-1$ durch $(1-\xi)$, aber nicht durch $(1-\xi)^2$ teilbar.

Daher teilt $(1-\xi)^{np-p+1}$ das Ideal $(x+y)$. Wir können also $(x+y) = \mathfrak{a}_0 (1-\xi)^{np-p+1}, (x+\xi y) = \mathfrak{a}_1 (1-\xi), \ldots, (x + \xi^{p-1} y) = \mathfrak{a}_{p-1}(1-\xi)$ schreiben, wobei die Ideale $\mathfrak{a}_0, \ldots, \mathfrak{a}_{p-1}, (1-\xi)$ nach Lemma 9.2 paarweise koprim sind. Somit ist

$$\mathfrak{a}_0 \cdots \mathfrak{a}_{p-1} = (z)^p.$$

Die $\mathfrak{a}_i$ sind Hauptideale und jeweils wegen der eindeutigen Faktorisierung von Idealen in Primideale die p-te Potenz eines Ideals. Da p regulär ist, ist $\mathfrak{a}_i$ für alle i die p-te Potenz eines Hauptideals $\mathfrak{b}_i$. Sei t_i ein Erzeuger von $\mathfrak{b}_i$ und sei $v_i \in \mathbf{Z}[\xi]^\times$ so, dass $x + y = v_0 (1-\xi)^{np-p+1} t_0^p$ und $x + \xi^r y = v_r (1-\xi^r) t_r^p$ für alle $1 \leq r \leq p-1$ gilt. Hier haben wir verwendet, dass $1 - \xi^r$ gleich $1 - \xi$ bis auf Multiplikation mit einer

Einheit ist (siehe Lemma 3.1). Weiter ist für alle $1 \leq r < s \leq p-1$:

$$\begin{aligned} v_r t_r^p - v_s t_s^p &= \frac{1}{(1-\xi^r)(1-\xi^s)}\big((1-\xi^s)(x+\xi^r y) - (1-\xi^r)(x+\xi^s y)\big) \\ &= \frac{1}{(1-\xi^r)(1-\xi^s)}\big((\xi^r-\xi^s)(y+x)\big) \\ &= v_0 \frac{(\xi^r-\xi^s)(1-\xi)}{(1-\xi^r)(1-\xi^s)}(1-\xi)^{(n-1)p} t_0^p \end{aligned}$$

und schliesslich:

$$t_r^p + v t_s^p = \left(\frac{v_0(\xi^r-\xi^s)(1-\xi)}{v_r(1-\xi^r)(1-\xi^s)}\right)(1-\xi)^{(n-1)p} t_0^p$$

mit $v := -\frac{v_s}{v_r}$. Als Produkt von Einheiten ist $u' := \frac{v_0(\xi^r-\xi^s)(1-\xi)}{v_r(1-\xi^r)(1-\xi^s)}$ selbst eine Einheit.

Seien nun $a, b \in \mathbf{Z}$ so, dass $t_r^p \equiv a \pmod p$ und $t_s^p \equiv b \pmod p$ ist. Also ist

$$a + vb \equiv u(1-\xi)^{(n-1)p} z^p \equiv 0 \pmod p,$$

da $n > 1$ ist. Man bemerke, dass $b \neq 0$ ist, da $b \equiv 0 \pmod p$ im Widerspruch dazu steht, dass $\mathfrak{a}_s$ nicht durch $(1-\xi)$ geteilt wird. Seien $\alpha, \beta \in \mathbf{Z}$ so, dass $\alpha b + \beta p = 1$ ist. Dann ist also $b \equiv \frac{1}{\alpha}$ und weiter $v \equiv \frac{a}{b} \equiv a\alpha \pmod p$. Daher ist v kongruent zu einer ganzen Zahl modulo p.

Kummers Lemma 7.1 gibt uns die Existenz einer Einheit $\varepsilon \in \mathbf{Z}[\xi]$, so dass $\varepsilon^p = v$ ist. Es ist also

$$t_r^p + (\varepsilon t_s)^p = u'(1-\xi)^{(n-1)p} t_0^p$$

und wegen der Induktionsvoraussetzung ist $t_0 t_r t_s = 0$. Dies impliziert, dass $z = 0$ ist, was aber ein Widerspruch zu $z \notin (1-\xi)$ ist; damit ist Satz 9.1 bewiesen.

Der Beweis des Satzes 9.1 ist im Grunde genommen der Originalbeweis von Kummer in [15]. Einzig für den Fall $n = 0$ ist Kummers Beweis etwas komplizierter und wir sind einer Vereinfachung gefolgt, wie sie zum Beispiel in [16] zu finden ist.

Korollar 9.4. *Sei p eine reguläre Primzahl und seien x, y, z ganze Zahlen, so dass*

$$x^p + y^p = z^p$$

gilt. Dann ist $xyz = 0$.

Beweis. Der Fall $p = 3$ wurde schon in Abschnitt 8 gezeigt. Wir können also $p \geq 5$ annehmen. Gesetzt, es sei $xyz \neq 0$. Indem wir durch den $\mathrm{ggT}(x, y, z)$ teilen, können wir annehmen, dass die Zahlen x, y, z teilerfremd sind. Wir ordnen die Gleichung $x^p + y^p = z^p$ so um, dass wenn xyz durch p teilbar ist, dann z durch p teilbar sei. Sehen wir die ganzen Zahlen x, y, z als Elemente von $\mathbf{Z}[\xi]$ an, können wir $z = u(1-\xi)^{(p-1)n} z_1$ mit $n \geq 0$, $u \in \mathbf{Z}[\xi]^\times$ und einem zu p teilerfremden $z_1 \in \mathbf{Z}$ schreiben. Also ist

$$x^p + y^p = u^p (1-\xi)^{(p-1)pn} z_1^p$$

und kein x, y, z_1 liegt in $(1-\xi)$. Dies aber ist ein Widerspruch zu Satz 9.1 und somit muss $xyz = 0$ sein. □

Nicht jede Primzahl ist regulär. Kummer definierte ursprünglich in [17] eine reguläre Primzahl als eine ungerade Primzahl p, welche die Zähler der Bernoullizahlen $B_2, B_4, ..., B_{p-3}$ nicht teilt. Dies ist

äquivalent zu unserer Definition von regulärer Primzahl. Da 37 den Zähler von B_{32} teilt, ist $p = 37$ nicht regulär. Es ist nicht bekannt, ob es unendlich viele reguläre Primzahlen gibt.

Dass die Fermatsche Vermutung für jeden Exponenten $n \geq 3$ gilt, wurde 1994 von Andrew Wiles bewiesen. Wir erwähnen dies erst ganz zum Schluss, um zu unterstreichen, dass es uns nicht um das Resultat an sich geht. Man mag einwenden, dass die Behauptung, dass es uns nur um das Resultat an sich ginge, konträr zur Aussage stehe, die wir zu Beginn des zweiten Abschnitts gemacht haben, nämlich dass wir möglichst direkt Kummers Beweis zu führen suchten. Doch dies war unvermeidlich, schliesslich sind manche Bücher über die algebraische Zahlentheorie mehr als fünfhundert Seiten stark und nicht zur Abendlektüre gedacht.

Die Lösung eines mathematischen Problems ist manchmal nicht so sehr interessant wegen der schliesslichen Entscheidung einer offenen Frage, sondern wegen der Theorie, die zur Lösung führt. Freilich ist Kummers Satz obsolet geworden, denn das Resultat liegt nun seit mehr als zwanzig Jahren allgemeiner vor. Doch ist es wirklich *an sich* von Belang, ob Fermats letzter Satz gilt oder nicht? Wir wissen nun, dass Fermats letzter Satz eine erstaunliche Verbindung mit der Taniyama-Shimura-Vermutung besitzt. Wenn wir dies ausser Acht lassen und bloss das Problem an sich betrachten: Hätte man mit Computern ein Gegenbeispiel gefunden, hätte dies irgendwas geändert?

Literatur

[1] M. Atiyah and I.G. MacDonald. *Introduction to Commutative Algebra.* Addison-Wesley Publishing Company, 1969.

[2] I. Schur, *Zur Irreduzibilität der Kreisteilungsgleichung*, Math. Zeit. 29 (1929), Seite 463

[3] N. Bourbaki. *Commutative Algebra Chapters 1-7.* Springer-Verlag, 1989.

[4] N. Bourbaki. *Algebra II, Chapters 4-7.* Springer-Verlag, 2003.

[5] J. Neukirch. *Algebraische Zahlentheorie.* Springer-Verlag, 1992.

[6] S. Lang. *Algebra.* Springer-Verlag, 2002.

[7] K. Uchida. *Class numbers of imaginary abelian number fields, I.* Tohoku Mathematical Journal, Second Series 23.1 (1971): 97-104.

[8] J. W. S. Cassels. *Local fields.* Cambridge-University Press, 1986.

[9] T. Bühler, D. Salamon. *Functional Analysis I.* Preprint, Version 11. Mai 2016.

[10] F. Guovea. *p-adic Numbers - An Introduction.* Springer-Verlag, 1997.

[11] J. W. S. Cassels, A. Fröhlich. *Algebraic Number Theory.* London Mathematical Society, 1967.

[12] E. Artin, J. Tate. *Class field theory.* Addison-Wesley Publishing Company, 1967.

[13] L. Euler. *Elements of Algebra.* Longman, Orme, and Co., 1840.

[14] G. Bergmann. *Über Eulers Beweis des grossen Fermatschen Satzes für den Exponenten 3.* Mathematische Annalen 164.2 (1966): 159-175.

[15] E. E. Kummer. *Allgemeiner Beweis des Fermatschen Satzes, da die Gleichung x... durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten..., welche ungerade Primzahlen sind und in den Zählern der ersten... Be..* Journal für die reine und angewandte Mathematik 40 (1850): 130-138.

[16] L. C. Washington. *Introduction Cyclotomic Fields.* Springer-Verlag, 1997.

[17] E. E. Kummer. *Zwei besondere Untersuchungen über die Classen-Anzahl und über die Einheiten der aus... ten Wurzeln der Einheit gebildeten complexen Zahlen.* Journal für die reine und angewandte Mathematik 40 (1850): 117-129.

[18] S. Lang. *Algebraic Number Theory.* Springer-Verlag, 1994.

[19] S. Lang. *Introduction to Cyclotomic Fields I and II.* Springer-Verlang, 1990.